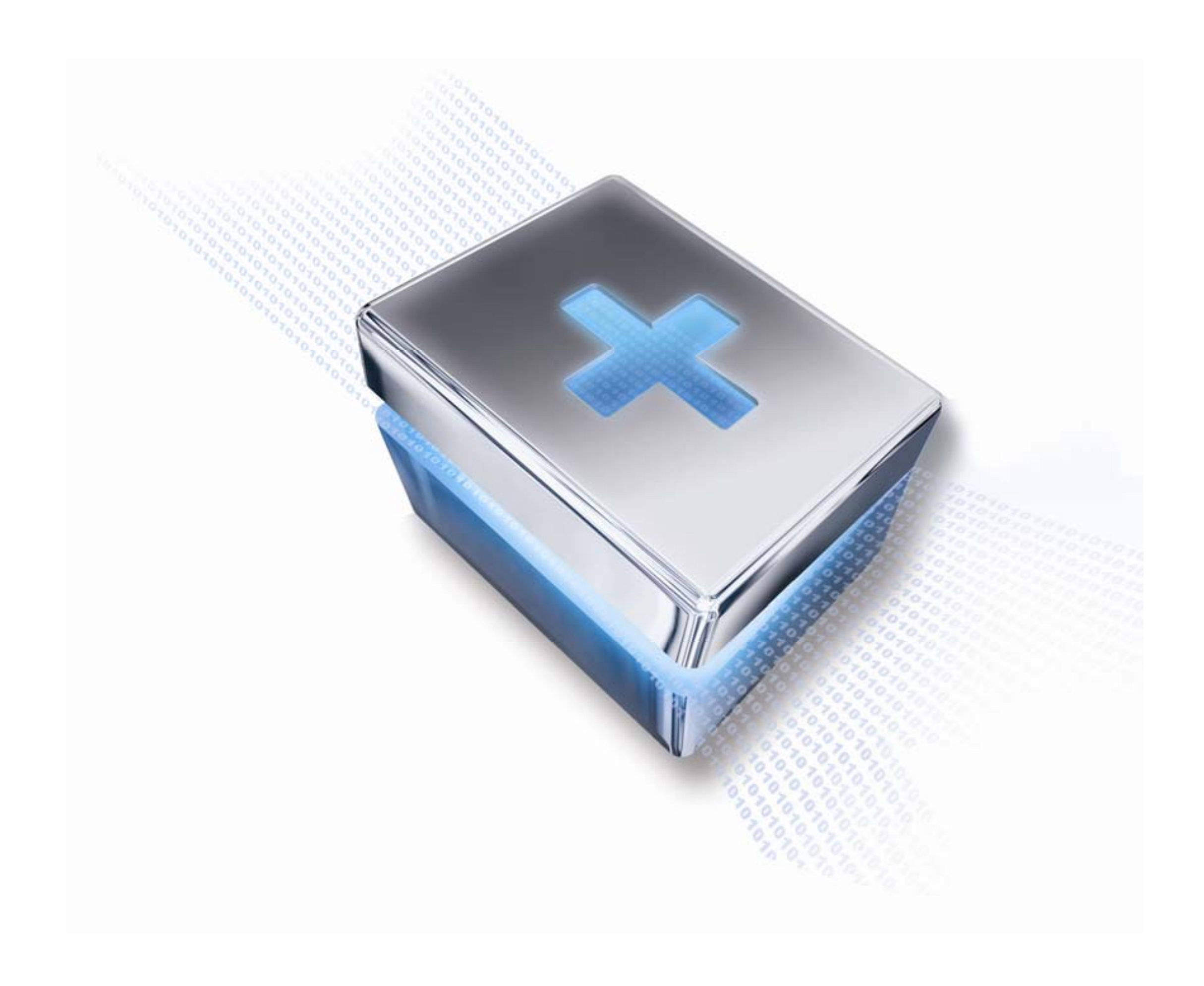


用戶手冊



目 錄

總裁致詞

首先感謝您選擇了北京金山軟體有限公司的產品！我們希望金山毒霸 V9.0 網路安全套裝在帶來全新殺毒感受的同時成為您電腦的最佳安全衛士！

今天金山毒霸 V9.0 網路安全套裝得以成功面市，我首先想感謝公司資訊安全及工具軟體業務群的全體研發人員，正是因為他們的不懈努力，我們才能成功地推出全新改版的具有更高品質的金山毒霸 V9.0 網路安全套裝。其次，我想感謝廣大的用戶。正是您們的支持，金山毒霸才能夠走到今天，並且在以後的道路上繼續為您們提供更好的產品服務。

金山毒霸自問世以來，以面向互聯網的強大防毒能力，眾多的功能套用、便捷的升級服務和強大的功能贏得大量用戶。

“做互聯網時代最好的殺毒軟體”是金山軟體反毒鬥士們一直努力的目標。我們深知這一目標的實現需要您的支援，我們成長的每一步都離不開您的幫助！所以，再次感謝您今天選擇了我們的產品！感謝您對金山軟體和中國正版軟體事業的支援！

公司介紹

金山軟體於1988年開始從事軟體產品的研發與銷售，目前是國內最知名的軟體企業之一，是中國領先的套用軟體產品和互聯網服務供應商。

多年來，金山一直不斷地為客戶帶來創新性的技術和產品，樹立了中國軟體產業耀眼的品牌。今天，金山產品線覆蓋了桌面辦公、資訊安全、實用工具、遊戲娛樂和行業套用等諸多領域，自主研發了適用於個人用戶和企業級用戶的WPS Office、金山詞霸、金山毒霸、劍俠情緣等系列知名產品。金山在套用軟體領域的技術實力和市場行銷能力方面一直保持著領先地位，營業規模持續增長。

金山通過了世界權威的CMM2級認證，建立了標準的軟體發展流程和品質體系，也通過ISO9001品質體系認證，建立起科學規範的供應鏈品質、生產、商務管理體系。這標誌著金山向規模化軟體企業的轉變。

目前，金山軟體的研發總部和行銷總部分別設立在珠海和北京，行銷網路已經遍佈全國。公司與日本、香港、臺灣等數十家代理商和全國數千家代理分銷網點擁有良好合作關係。公司通過OEM方式與聯想、方正、同方、TCL、IBM、DELL、HP、NOKIA等國際、國內知名IT企業建立了合作關係。金山已經發展成為大型專業化軟體公司。

金山軟體，與中國軟體產業共同進步！

第一章　前言

歡迎您使用金山毒霸 V9.0 網路安全套裝，請您仔細閱讀以下資訊：

金山毒霸 V9.0 網路安全套裝應包括以下內容:

- 金山毒霸 V9.0 網路安全套裝安裝光碟一張
- 簡易用戶手冊一本
- 金山毒霸正版用戶服務卡的序列號卡

金山毒霸注意事項：

本卡僅適用於金山毒霸 V9.0 網路安全套裝，僅授權在一台電腦中使用；在安裝《金山毒霸 V9.0 網路安全套裝》過程中，按照系統提示輸入卡上的金山序列號，便可享受升級服務；如您購買時發現塗層已經刮開，請勿購買。本卡塗層一經刮開，恕不退貨；請您妥善保管此卡，以便遺忘後找回。 如果您購買的金山毒霸 V9.0 網路安全套裝缺少上述任何一種物品，請及時與當地供應商聯繫。

信譽保證

如果您在使用過程中發現了什麼問題，請及時撥打金山毒霸技術支援熱線電話（電話：852-26114144）或登錄客服網站http://www.duba.com.hk或查詢解決方法。如果您對我們的產品有什麼意見或建議，請一定不吝指教，以便我們不斷改進。

版權聲明

、KINGSOFT®、是金山軟件享有權力的商標，本文中涉及到的其他產品名稱和品牌為其相關公司或組織的商標或注冊商標，特此鳴謝。

未得到北京金山軟體有限公司的正式許可，任何人或組織均不得以任何手段與形式對本手冊內容進行複製或傳播。

對於本手冊中的內容，北京金山軟體有限公司擁有最終的解釋權。

感謝您支持金山！

金山軟體最終用戶許可協定

========================

請務必仔細閱讀和理解本金山軟體最終用戶許可協定（《協定》）中規定的所有權利和限制。在安裝時，您需要仔細閱讀並決定接受或不接受本《協議》的條款。除非或直至您接受本《協議》的條款，否則本軟體不得安裝在您的電腦上。

作為參考，您現在就可以從本頁起列印出本《協定》的文本，或者參閱本“軟體”“幫助”檔中本《協議》的副本。

本《協定》是您與金山公司之間有關隨附本《協定》的金山軟體的法律協定。本軟體包括隨附的電腦軟體，並可能包括相關文檔印刷材料。您一旦安裝本“軟體”，即表示您同意接受本《協議》各項條款的約束。如您不同意本《協議》中的條款，您則不可以安裝或使用本“軟體”。

本“軟體”受著作權法及國際著作權條約和其他知識產權法和條約的保護。本“軟體”權利只許可使用，而不出售。

一・金山公司將本軟體在香港地區、澳門地區、臺灣地區的非專有的使用權授予您。 您可以：
1. 在一台電腦、工作站、終端機、掌上型電腦或其他數位電子儀器（“電腦”）上安裝、使用、顯示、運行（“運行”）本“軟體” 的一份副本。
2. 為了防止複製品損壞而製作備份複製品。這些備份複製品不得通過任何方式提供給他人使用，並在您喪失該合法複製品的所有權時，負責將備份複製品銷毀。
3. 為了把該軟體用於實際的電腦套用環境或者改進其功能、性能而進行必要的修改；但是，除合同另有約定外，未經金山公司許可，不得向任何第三方提供修改後的軟體。

二・您保證：
1. 不在本協議規定的條款之外，使用、複製、修改、租賃或轉讓本軟體或其中的任一部份。
2. 只在一台電腦上使用本軟體；一份“軟體”許可不得在不同電腦共同或同時使用。
3. 只在以下之一前提下，將本系統用於多用戶環境或網路系統上：
本“軟體”明文許可用於多用戶環境或網路系統上；
使用本“軟體”的每一節點及終端都已購買使用許可。
4. 不得對本“軟體”進行反向工程、反向編譯或反彙編。
5. 不出租、租賃或出借本“軟體”產品。
6. 在本“軟體”的所有副本上包含所有的版權標識。

三・軟體轉讓
您可將您在本《協議》項下的所有權利作永久性一次轉讓，轉讓後您的許可權即自行終止。轉讓的條件是：
1. 您不得保留副本；
2. 轉讓“軟體產品”（包括全部元件、媒體及印刷材料，任何升級版本和本《協定》）的所有部分；
3. 受讓人接受本《協議》的各項條款；
4. 如果“軟體產品”為升級版本，任何轉讓必須包括本“軟體產品”的所有前版本；

四・支援服務
1. 金山公司為您提供與“軟體”有關的支援服務（“支援服務”）。
2. 支援服務的使用受用戶手冊或其他金山公司提供的材料中所述的各項政策和計畫的制約。
3. 提供給您作為支援服務的一部分的任何附加軟體代碼應被視為本“軟體”的一部分，並須符合本《協議》中的各項條款。

4.　您提供給金山公司作為支援服務的一部分的技術資訊，金山公司可將其用於商業用途，包括產品支援和開發。除了在為您提供支援時必須的情況外，金山公司在使用這些技術資訊時不會以個人形式提及您。

五・軟體的替換、修改和升級

1.　金山公司保留在任何時候通過為您提供本“軟體”的替換版本或修改版本或這類升級版本以替換、修改或使本“軟體”升級的權利和為這類替換、修改或升級收取費用的權利。

2.　金山公司提供給您的本“軟體”的任何替換版本或修改軟體代碼或升級版本，將被視為本“軟體”的一部分並且要受到本《協議》條款的制約（除非本《協定》被隨附本“軟體”的替換或修改版本或升級版本的另外一份《協議》取代）。

3.　如果金山公司提供本“軟體”的一個替換或修改版本或任何升級版本，則（a）您對本“軟體”的繼續使用條件是您接受本“軟體”的這類替換或修改版本或升級版本以及任何隨附的取代《協議》，並且（b）就替換或修改版本的“軟體”而言，您對“軟體”的所有先前版本的使用將被終止。

六・權利的保留：

未明示授予的一切其他權利均為金山公司所有。

七・本“軟體”的著作權

1.　本“軟體產品”及其所有複製品的名稱，與光碟上或本軟體中注明的公司同在。

2.　本“軟體產品”（包括但不限於本“軟體”中所含的任何圖像、照片、動畫、錄影、錄音、音樂、文字和附加程式）、隨附的印刷材料、及本“軟體”任何副本的著作權，均由金山公司擁有。

3.　本軟體及文檔享有版權，並受國家版權法及國際協約條款的保護。

4.　您不可以從本軟體中去掉其版權聲明；並保證為本軟體的複製品（全部或部分）複製版權聲明。您同意制止以任何形式非法複製本軟體及文檔。

5.　您不可複製本“軟體”隨附的印刷材料。

八・出口限制

您同意不將本“軟體”、其任何部分或任何屬“軟體”的直接成果的任何程式或服務出口或轉口給香港地區、澳门地區、臺灣地區以外的任何國家或者地區。

九・售後擔保：

1.　金山公司擔保，在正常使用的情況下，自售出之日起九十天內，其軟體載體無材料或工藝缺陷。經驗證確有缺陷時，金山公司的全部責任就是退換其軟體載體作為對您的補償。

2.　因事故、濫用或錯誤套用導致的載體缺陷，售後擔保無效。

3.　退換的載體享受原擔保期剩餘時間，或三十天的擔保；取其長者優先。

4.　除上述之外，本軟體不享受任何其他形式的售後擔保。

十・責任有限：

您及金山軟體均認可病毒、惡意程式等的產生、傳播存在不可控制性及不可預見性，因此金山軟體僅保證在其技術水準許可範圍內及其已掌控病毒範圍內提供本軟體病毒查殺服務，金山軟體不就任何其尚未掌控的病毒、惡意程式等作任何保證，但金山軟體將致力于不斷提升公司技術水準及掌控病毒範圍。您已經明確知悉所述情況，並承諾不就因此而可能造成的任何結果向金山軟體主張權利。

上述擔保，無論是明示或暗喻的，為擔保的全部內容，包括對特殊套用目的的商品性和適應性擔保。在適用法律所允許的最大範圍內，金山公司或其供應商絕不就因使用或不能使用本“軟體”所引起的或有關的任何間接的、意外的、直接的、非直接的、特殊的、懲罰性的或其他任何損害賠償（包括但不限於因人身傷害或財產損壞而造成的損害賠償，因利潤損失、營業中斷、商業資訊的遺失而造成的損害賠償，因未能履行包括誠信或相當注意在內的任何責任致使隱私洩露而造成的害賠償，因疏忽而造成的損害賠償，或因任何金錢上的損失或任何其損它損失而造成的損害賠償）承擔賠償責任，即使金山公司或其任何供應商事先被告知該損害發生的可能性。即使補救措施未能達到預定目的，本損害賠償排除條款將仍然有效。

十一・許可終止：

1. 如您未遵守本《協議》的各項條款和條件，在不損害其他權利的情況下，金山公司可終止本《協議》。終止《協議》時，您必須立即銷毀本軟體的所有複製品，或者歸還給金山公司。

2. 通過向您提供本“軟體”或本“軟體”的任何替換或修改版本或升級版本的一份取代《協議》，並規定您繼續使用本“軟體”或這類替換、修改或升級版本的條件是您接受這類取代《協議》，金山公司可以終止本《協議》。

十二・適用、管轄法律：

本協定適用《中華人民共和國著作權法》、《中華人民共和國電腦軟體保護條例》、《中華人民共和國商標法》、《中華人民共和國專利法》等法律法規。

本《協定》受中華人民共和國法律管轄。

十三・特別提示：

為了不斷提高本“軟體”和服務的品質，我們將有可能搜集您對本軟體進行使用的資訊，並不定期地予以回饋。我們不會搜集您的姓名、位址、聯繫方式等個人資訊以及檔內容等涉及資訊安全的資訊。以上搜集的資訊僅僅為了市場分析需要，以便我們今後能夠為您提供更好的功能和服務，金山公司對此資料嚴格保密。

本條所指搜集訊息的範圍以金山軟體適時的技術水準為判斷標準。金山軟體將盡最大努力力求判斷的準確性，但因受到現實技術水準等的限制，金山軟體僅依照自有的判斷能力進行甄別收集。您已明確知悉上述內容，且認可金山軟體的操作，願意承擔因此而可能造成的損失。

至此，您肯定已經詳細閱讀並已理解本協議，並同意嚴格遵守各條款和條件。

第二章 安裝和卸載

2.1 系統資源要求

在安裝金山毒霸 V9.0 網路安全套裝前您的電腦必須安裝帶有如下配置的作業系統。

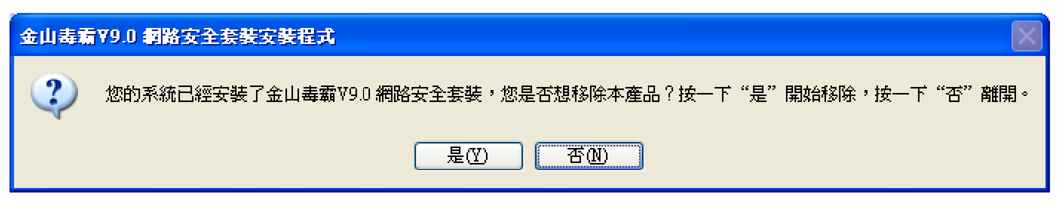
2.2 安裝前的準備

設定	說明
作業系統	Windows 2000 Professional Windows XP Professional（32 位） Windows XP Home Edition （32 位） Windows Vista（32 位）（Windows Vista Starter 版本不支援）
CPU	Pentium3 / Pentium 4
記憶體	512M
硬碟	至少 150MB 可用硬碟空間
視頻	1024x768，增強色 16 色（含）以上
IE	5.0.2314 或更高版本的 IE

2.3 安裝導航

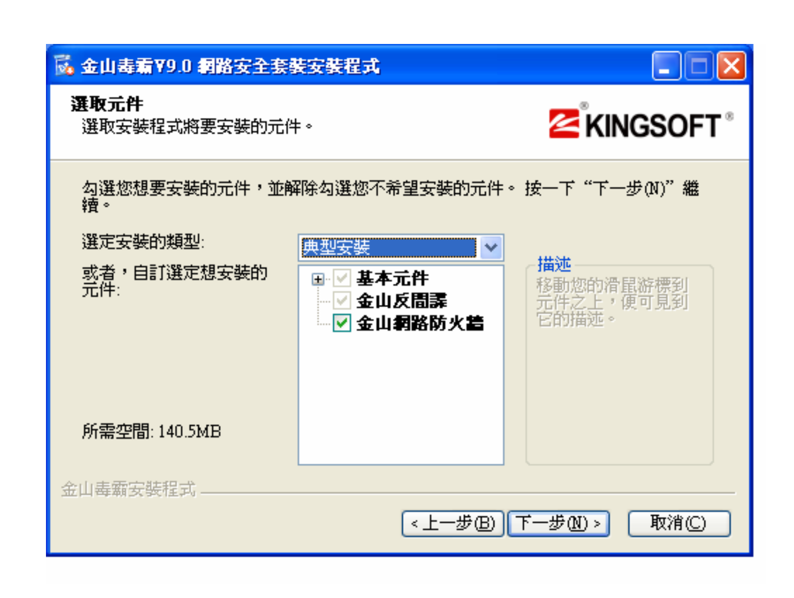
將安裝光碟插入光碟機，安裝導航自動進行系統配置和安裝準備工作。如果您停止了光碟自動播放功能，請用 檔案管理器瀏覽光碟，雙擊 "fscommand\KIS9CHT.EXE" 即可。

如果您已經安裝了其他版本的金山毒霸，那麼安裝程式將首先卸載以前的版本，再安裝金山毒霸 V9.0 網路安全套裝；如果是首次選用金山毒霸，可直接安裝。按照安裝導航提示，可輕鬆完成。



請仔細閱讀金山軟體最終用戶許可協定，確認後，單擊 "我接受" ；如果您不接受該協議，單擊 "取消" ，退出安裝程式。

在 "安裝類型" 中，預設為典型安裝，表示系統將金山毒霸殺毒套裝的基本元件，包括金山毒霸 V9.0、金山網路防火牆 V9.0、金山反間諜 V9.0 安裝到您的電腦中。您也可以自定義選擇安裝元件。點擊 "下一步" 繼續。

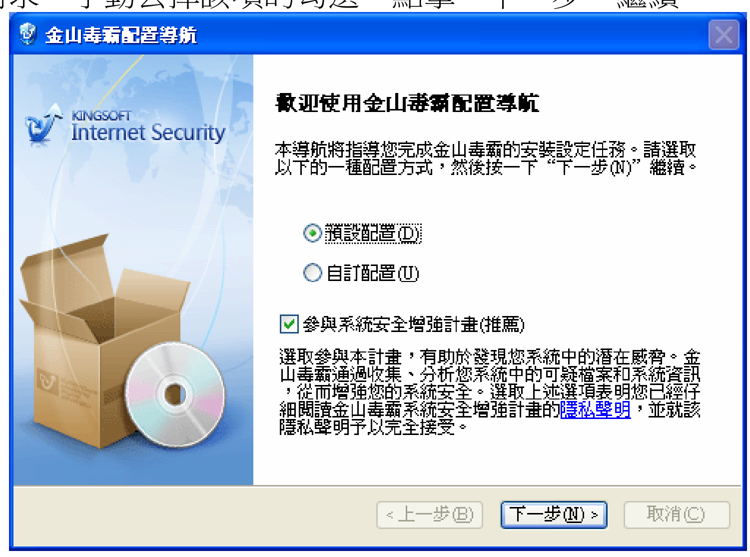


接下來選擇安裝位置，請你根據您的需要，選擇金山毒霸 V9.0 網路安全套裝的存放路徑，點擊“下一步”繼續。

在確認安裝元件頁面中，查看當前設定，並點擊“安裝”，安裝程式將開始複製檔。

【注意】：在安裝過程中，點擊“取消”，則退出整個安裝過程。

檔案複製完成，點擊“下一步”，進入金山毒霸 V9.0 網路安全套裝的配置導航，您可選擇預設配置，也可根據自己的需要選擇自定義配置。系統預設勾選“參與金山毒霸系統安全增強計畫”，該計畫將收集您系統中存在潛在風險的資料上報給金山公司，您也可以根據需求，手動去掉該項的勾選。點擊“下一步”繼續。



隨後進入內存查毒，強烈建議不要跳過此過程。

進入註冊時必須驗證的元件及服務頁面，驗證完畢，安裝完成，點擊“完成”將啟動線上升級程式。

點擊“完成”後，進入線上升級，升級過程詳見“升級篇”。

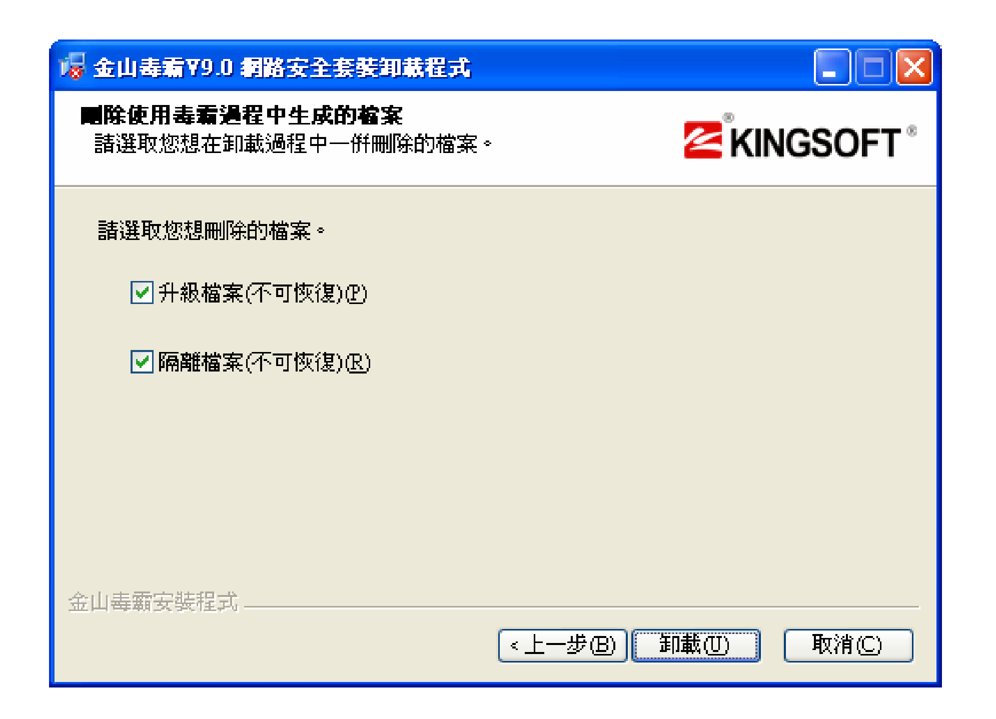
2.4 卸載

【注意】：執行卸載前，請先退出金山毒霸程式。請不要直接刪除金山毒霸安裝目錄，否則將導致系統運行不正常。

★ 方法一：請於“開始”|“所有程式”|“金山毒霸 V9.0 網路安全套裝”功能表中執行“卸載金山毒霸殺毒套裝” 命令，卸載程式將指引您乾淨、安全的卸載金山毒霸 V9.0 網路安全套裝 。

【注意】：點擊“取消”按鈕， 將取消本次卸載操作。

程式提示您選擇要刪除的檔，包括日誌檔，升級檔和隔離檔，同時您也可以參與我們的產品改善計畫調查，選擇完畢，點擊“卸載”。卸載嚮導關閉毒霸正在運行的程式，卸載元件及服務並清除註冊表，然後進入卸載檔步驟。



【注意】：卸載進度一旦開始，某些檔就會相應被刪除，故不提倡中途取消操作。

卸載進度完成，程式提示重啟電腦。

【注意】：強烈建議馬上重啟電腦，這樣才能完成全部檔的卸載過程。重啟之前，請保存好您所有打開視窗的檔，然後點擊“完成” 。

★ 方法二： 點擊“開始”|“設定”|“控制面板” ，並在控制面板裏面執行“添加或刪除程式” ，繼而在彈出的對話方塊中選擇“金山毒霸 V9.0 網路安全套裝”並單擊其右邊的“修改/刪除”即可，餘下的卸載操作同方法一。

第三章　金山毒霸 V9.0

3.1 入門篇

3.1.1 主要功能

金山毒霸 v9.0 是一款功能強大、方便易用的個人及家庭首選反病毒產品之一，它能保護您的電腦免受病毒、駭客、垃圾郵件、木馬和間諜軟體等等網路危害。

★金山毒霸 V9.0 網路安全套裝**兩大功能亮點：**

✓ **三維互聯網防禦體系**

金山毒霸 V9.0 網路安全套裝對病毒和木馬等威脅的查殺，採取本地病毒庫掃描、惡意行為攔截和可信認證技術的三重防護。

✓ **一對一安全診斷**

金山毒霸 V9.0 網路安全套裝對用戶系統中多達 1000 項的關鍵區域進行掃描，結合可信認證技術以及各類監控狀態判斷，從而智慧判斷當前用戶系統的安全性。

★金山毒霸 V9.0 網路安全套裝 **主要功能：**

✓ **搶殺技術**

搶殺技術確保在系統啟動早期，清除各類病毒、木馬、惡意軟體等威脅，讓各種威脅在發作前就徹底被清除乾淨。

✓ **集成金山反間諜**

金山毒霸 V9.0 網路安全套裝殺毒套裝集成金山反間諜，具備金山反間諜所有功能，金山毒霸與金山反間諜聯合對系統進行診斷，給用戶更為準確的系統網路安全指數，作為您系統是否安全的權威參考。提供方便實用的隨身碟病毒免疫工具、進程管理器 、LSP 修補工具、歷史痕跡清理和垃圾檔案清理多款小工具。

✓ **系統安全增強計畫**

本計畫將對潛在系統中的危險程式或具有可疑行為的執行程式，進行分析並做出相應的處理策略。它有助我們更迅速的應對未知危險程式，增強用戶系統的安全性。

✓ **網頁安全防禦**

在您瀏覽網頁的時候，網頁安全防禦馬將監控網頁行為並阻止通過網頁漏洞下載的木馬程式威脅您的系統安全。

✓ **主動漏洞修補**

根據微軟發佈的補丁，第一時間提供最新漏洞庫，通過自動升級後自動幫助用戶打上新發佈的補丁。

✓ **主動攔截惡意行為**

對具有惡意行為的已知或未知威脅進行主動攔截，有效地保護系統安全。

✓ **主動即時升級**

主動即時升級每天自動幫助用戶及時更新病毒庫，讓您的電腦能防範最新的病毒和木馬等威脅。

✓ **全面相容 Windows Vista**

能夠全面相容 Windows Vista 作業系統，為用戶提供基於微軟最新作業系統的全面防護服務。

✓ **查殺病毒、木馬、惡意軟體**

使用資料流程、脫殼等一系列先進查殺技術，打造強大的病毒、木馬、惡意軟體查殺功能，將藏身於系統中的病毒、木馬、惡意軟體等威脅一網打盡，保障用戶系統安全。

✓ 駭客防火牆

金山網路防火牆，根據個人上網的不同需要，設定安全級別，有效的提供網路流量監控、網路狀態監控、IP 規則編輯、套用程式訪問網路許可權控制，駭客、木馬攻擊攔截和監測等功能。

3.1.2 主介面介紹

訪問金山毒霸 V9.0，請執行下列任一操作：

✓ 在桌面雙擊“金山毒霸”圖示。



✓ 在 Windows 任務欄中狀態欄雙擊金山毒霸的小圖示“ ”或右鍵單擊該圖示，在彈出的功能表中選擇“打開金山毒霸”。

✓ 在 Windows 2000 任務欄中，單擊“開始→程式→金山毒霸 V9.0 網路安全套裝→金山毒霸 V9.0”。

✓ 在 Windows XP 任務欄中，單擊開始→所有程式→金山毒霸 V9.0 網路安全套裝→金山毒霸 V9.0。

✓ 在 Windows Vista 任務欄中，單擊開始→程式→金山毒霸 V9.0 網路安全套裝→金山毒霸 V9.0。



✓ **菜單欄**：採用Windows標準風格，單擊其中任何一項功能表，即可彈出詳細的下拉功能表，您可以方便、快捷地選定您所需的功能功能表。

✓ **標籤欄**：包括兩個活動標籤“安全起點站” 和“監控和防禦” 。預設啟動“安全起點站” ，您可以根據自身需要切換活動標籤，同一時間有且只有一個活動標籤。

➢ 安全起點站

金山毒霸 V9.0 的安全起點站頁面包括查殺病毒木馬、安全建議和服務狀態。

查殺病毒木馬

快捷方式：您可以直接雙擊掃瞄任務中的“我的電腦”、“我的文檔”和“移動設備”進行相應的病毒查殺作業。或者單擊上述的掃瞄任務，再按一下“查殺病毒/木馬”按鈕，進行同樣的查殺作業。

指定路徑：您也可以按一下“指定路徑”，直觀地選取需要進行病毒查殺的具體位置，再按一下“查殺病毒/木馬”按鈕，進行查殺作業。

安全建議 根據您的電腦當前是否已啟動毒霸的監控功能、是否已使用金山序列號、是否已升級到最新的病毒庫，安全診斷區域會準確地判定為三種安全級別：安全、有風險、危險
安全： 當您已經將金山毒霸 V9.0 全部監控都開啟，系統安全狀況良好，並使用有效金山序列號，病毒庫已更新至最新時，則判定為安全狀態。



有風險： 當您的金山毒霸 V9.0 部分監控未被開啟，或病毒庫未更新至最新，或系統狀況不是很好時，判定為風險狀態。



危險： 當您的金山毒霸 V9.0 大多數或全部監控都未開啟，或病毒庫過舊，或沒有使用金山序列號，或系統安全狀況比較差，則判定為危險狀態。



服務狀態 顯示您的金山毒霸 V9.0 當前所用的序列號號，以及最後的升級時間和服務到期時間，您可以在此處更換序列號。

➢ 監控和防禦

金山毒霸 V9.0 的監控和防禦頁面包括監控、防禦和服務三大功能。您可以在頁面右側根據需要對各項進行啟動或關閉作業;也可以按一下“詳細設定”進入“金山毒霸—綜合設定”區進行防毒設定;並可以按一下“檢視日誌”進入“金山毒霸日誌檢視器”檢視詳細的歷史記錄 。



監控：包括檔案即時監控和郵件監控。

檔案即時防毒：啟動後自動在後臺執行，從開機起全程監控，徹底防止病毒以及其他威脅入侵。

郵件監控：幫助用戶監控每一封接發郵件是否攜帶病毒，並及時處理帶毒郵件。

防禦：包括網頁安全防禦和惡意行為攔截。

網頁安全防禦：啟動後將在您瀏覽網頁時監控網頁行為，並阻止惡意行為威脅系統安全。

惡意行為攔截：啟動後將對已知或未知的惡意威脅進行攔截，有效保護系統安全。

服務：包括主動即時升級和主動漏洞修補。

主動即時升級：啟動後將每天主動更新您的病毒庫，使電腦能防範最新的病毒和木馬威脅。

主動漏洞修補：定期自動更新您的系統補丁，使您的系統減少被攻擊的可能。

3.2 查殺病毒篇

3.2.1 常見掃描方式及其設定

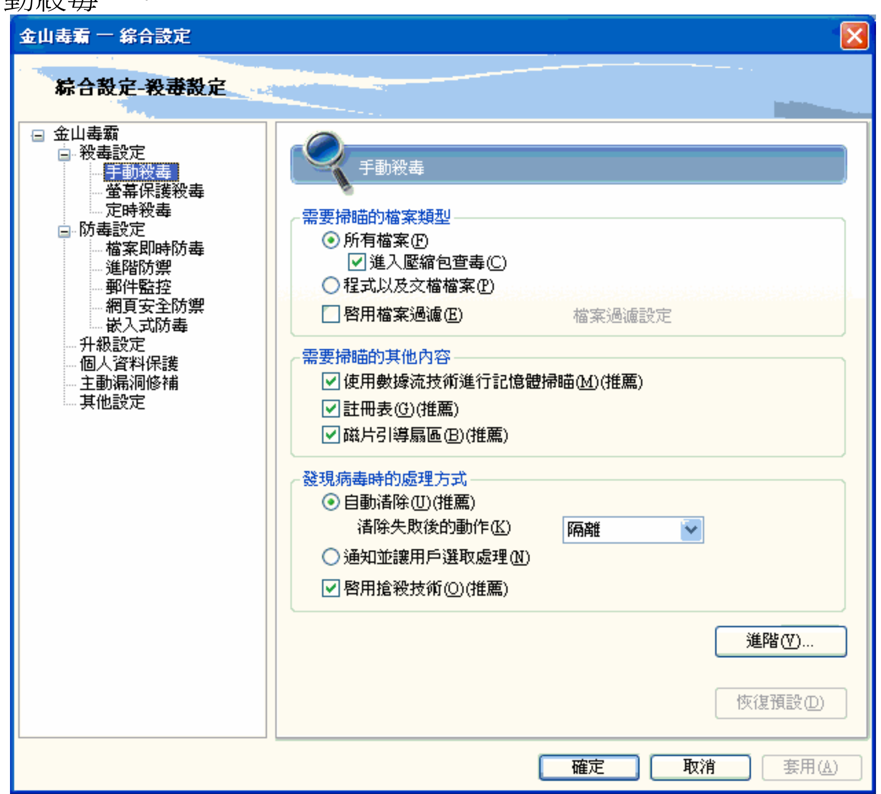
3.2.1.1 手動殺毒

在金山毒霸 V9.0 的安全起點站頁面 選擇需要查殺的範圍，點擊“查殺病毒木馬”按鈕，即可對您選擇的檔案 夾進行殺毒，或點擊功能表欄的操作→查殺病毒木馬，即可啟動對電腦的查殺。掃描結束，如果發現用戶的系統中存在風險程式，彈出風險程式處理介面，請點擊“清除”。清除完成，彈出查毒報告。在此頁面，您可以點擊“完成”，或者點擊“查看詳細日誌”查看查毒記錄。



手動殺毒設定

首先在功能表欄選擇：“工具”|“綜合設定”命令，然後於其中的“殺毒設定”中選定“手動殺毒”。



各選項說明如下：

- ✓ **需要掃描的檔類型：**選定在掃描時檢查的檔類型和內容，預設推薦掃描所有檔並進入壓縮包查毒，您可在檔過濾設定中進行過濾檔副檔名以及過濾路徑的設定。
- ✓ **需要掃描的其他內容：**包括磁片主引導記錄，引導磁區，註冊表以及記憶體記錄，預設全選。
- ✓ **發現病毒時的處理方式：**包括通知並讓用戶選擇處理以及自動清除，預設發現病毒自動清除，清除失敗則將檔隔離。
- ✓ 預設開啟搶殺技術。

清除失敗後處理方式如下：

- ➢ **隔離：**自動將染毒檔添加到病毒隔離系統；
- ➢ **跳過：**僅通知用戶，不對染毒檔做任何操作。

✓ **高級設定：**單擊介面中的“高級”，彈出高級設定頁面，包括清除病毒設定和未知病毒檢測。預設推薦清除病毒前將檔備份至隔離區、清除壓縮包內的病毒、掃描風險程式和啟用資料流程查毒。您也可以選擇啟用精細查毒模式，但這樣可能會降低查毒的速度。

【注意】：每次修改設定，請務必點擊“套用”，保存該次設定至下一次修改。

3.2.1.2 右鍵查殺

“右鍵方式殺毒”是金山毒霸一直沿用的傳統殺毒功能。選中一個檔案或檔案夾，單擊滑鼠右鍵，於彈出的功能表中選擇“使用金山毒霸進行掃描”，馬上對您選定的所有檔或檔夾進行手動殺毒操作，讓您殺毒更方便、快捷！

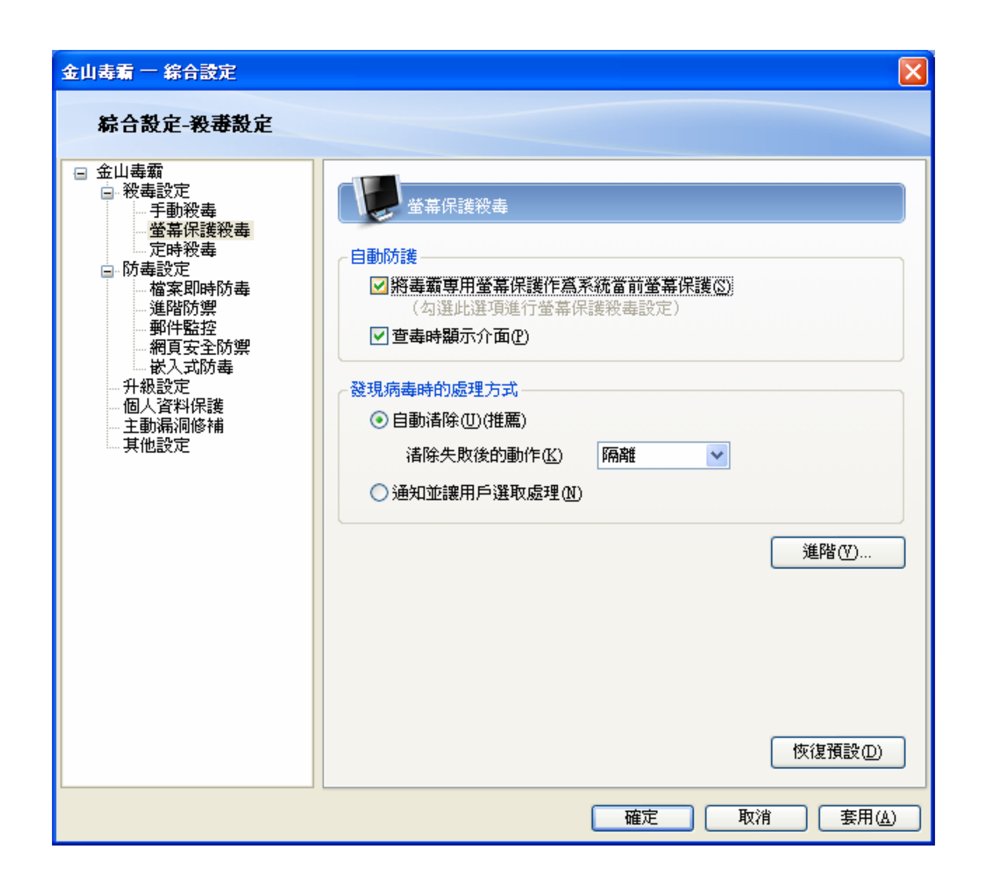
3.2.1.3 螢幕保護查殺

金山毒霸正在進行螢幕保護殺毒... (已執行 1 分鐘，15:43:49)
掃瞄: C:\... Reader 8\Data1.cab_582E4EC531D94B91B2C5CEA716411539
已掃瞄: 2703
感染: 0
處理: 0

螢幕保護查殺充分利用電腦空閒時間，在不影響用戶工作的情況下，確保用戶電腦免受病毒之害。程式一直運行在後臺，一旦金山毒霸螢幕保護查殺被啟動，便自動啟動病毒掃描程式對當前硬碟所有分區進行隨機病毒掃描。屏保結束時中止查毒，並彈出殺毒結果的對話方塊，是典型的“居安思危”的好幫手！

螢幕保護查殺設定

首先點擊金山毒霸 V9.0 與 主介面功能表欄的工具，選擇“綜合設定”命令，然後於其中的“殺毒設定”中選定“螢幕保護查殺”即可。



具體設定選項包含自動防護、發現病毒時的處理方式和高級選項。

- ✓ **自動防護**：手動勾選開啟屏保殺毒，方能實現屏保查毒；預設在後臺運行，當您選擇查毒時顯示介面，才運行於前臺。
- ✓ **發現病毒時的處理方式**：您可選擇接收通知並自主選擇處理方式，預設為自動清除。
- ✓ **清除失敗的處理方式**：預設是當發生清除失敗時，將檔放到隔離區；您也可以選擇"跳過"的處理方式。
- ✓ **進階設定**：預設是清除病毒前將檔備份到隔離區，和處理壓縮包內的病毒。您也可根據需要，進行篩選。

3.2.1.4 定時殺毒

金山毒霸的"定時殺毒"功能，可以自動執行用戶事先定制的任務，達到事半功倍的效果。



✓ 設定打開方式：

點擊金山毒霸 V9.0 主介面功能表欄的工具→綜合設定→殺毒設定→定時殺毒。

載入選項：

➢ **啟動定時殺毒：**勾選 “啟動定時殺毒”後，即按指定的方案執行掃描（如不勾選此項，方案設定將反灰不可選）。

方案設定：

➢ **一次性：**請在“開始日期”以及“開始時間”中定制具體掃描的時間。

➢ **每天：**請在“開始日期”和“開始時間”中定制開始的日期、時間，並預設每天在此時執行查毒任務。

➢ **每週：**請在“每週”後的下拉清單中選擇，並在“開始日期”和“開始時間”中定制開始的日期、時間，預設每週將在此對應的日期、時間執行查毒任務。

➢ **每月：**請在“每月”後的下拉清單中選擇，並在“開始日期”和“開始時間”中定制開始的日期、時間，預設每月將在此對應的日期、時間內執行查毒任務。（若選擇月末執行，遇到某月末無日期，則自動跳到下一月該日期、時間執行，如定制開始日期為 2007 年 1 月 31 日、開始時間為 9：20，則在 2007 年 3 月 31 日 9：20 再次執行掃描任務）。

3.3 預防病毒篇

3.3.1 檔案即時防毒

金山毒霸檔案即時防毒可以監控對檔的一切操作,發現並攔截帶毒檔案的訪問並停止該檔訪問的進程活動。檔案即時防毒啟動後,駐留記憶體,自動運行于後臺,在任一套用程式對檔案進行操作;在接收電子郵件、從網路下載或 QQ、MSN 傳遞檔案、打開光碟時進行病毒監控,徹底防止病毒入侵。如果發現病毒,將根據其屬性設定採取相應措施。

啟動:

方法一:開機時自動啟動

在金山毒霸 V9.0 主介面中選擇"監控和防禦"頁面,開啟"檔即時防毒;或者在"綜合設定"中選擇"防毒設定"→"檔即時防毒",勾選"開機自動運行檔即時防毒",即可。

方法二:通過金山毒霸最小化圖示啟動

右鍵單擊 Windows 任務欄中狀態欄的程式圖示"",選中"打開檔即時防毒"即可。啟動後,任務欄中狀態欄的程式圖示變為""。

退出:

方法一:通過右鍵功能表停止

右鍵單擊任務欄中狀態欄的程式圖示"",在功能表列表中,選擇"關閉檔案即時防毒"即可,任務欄中狀態欄的程式圖示變為"",表示檔案即時防毒已關閉。

方法二:通過監控和防禦頁面

於主介面中選擇"監控和防禦"頁面,然後選定"檔案即時防毒",點擊右側活動頁面中的"關閉"按鈕即可。

檔案即時防毒綜合設定

首先切換到監控和防禦頁面,選擇"檔案即時防毒",再點擊"詳細設定",然後於"防毒設定"項中選定"檔案即時防毒"。

各選項說明如下:

✓ **自動防護:**您在此可以設定開機自動執行檔案即時防毒,設定後即允許金山毒霸隨系統啟動而開啟對檔案的即時防毒。

✓ **需要檢查的檔案類型:**您在此可以對需要即時防毒監控的檔案類型進行設定,系統預設設定為所有檔案。

✓ **發現病毒時的處理方式:**對監控下發現的病毒木馬檔,預設設定為"自動清除",您也可選擇"禁止訪問"將其隔離起來。

啟動搶殺技術:啟動搶殺技術,可以確保在系統啟動之前,徹底清除所有病毒、木馬、惡意軟體等威脅,讓各種威脅在發作前就徹底被清除乾淨。

清除失敗後處理方式如下:

- **隔離:**自動將染毒檔案添加到病毒隔離系統;
- **跳過:**僅通知用戶,不對染毒檔案做任何操作。這並不能解決問題。在下次執行相同操作時還會得到警報。

✓ **進階選項:**定制清除病毒設定和未知病毒檢測。預設清除病毒前備份檔案至隔離區,如果用戶選擇精細查毒模式,查毒的速度會有所降低。

3.3.2 進階防禦

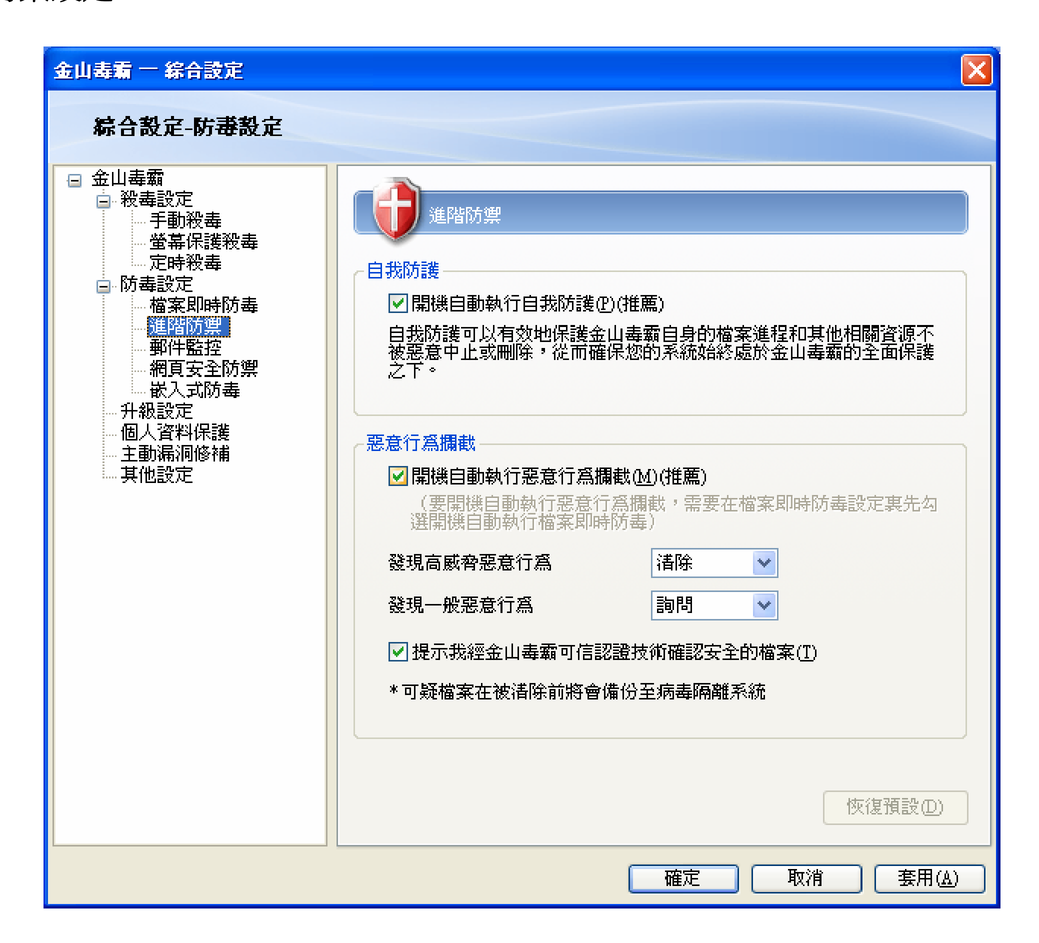
金山毒霸 V9.0 的自我保護及惡意行為檢測功能對網路駭客傳播的一些專門針對殺毒軟體的病毒及啟發性地對相關惡意技術能作出準確的檢測，保護金山毒霸的病毒查殺和監控程序的正常運作，防止您的電腦受到侵襲。

打開方法：

方法一：在金山毒霸 V9.0 主介面“監控和防禦”頁面，點擊“惡意行為攔截”→“詳細設定”，選擇“防毒設定”→“進階防禦”；

方法二：在金山毒霸 V9.0 主介面功能表欄，點擊“工具”。在下拉功能表中，選擇“綜合設定”→“防毒設定”→“進階防禦”；

進階防禦設定



各選項說明如下：

✓ **自我防護：**預設勾選開啟自我防護。你也可以根據您的需要，對該預設項進行修改。開啟自我防護，可以有效保護金山毒霸自身的檔進程和其他相關資源不被惡意中止或刪除，從而確保您的系統始終處於金山毒霸的全面保護之下。

✓ **惡意行為攔截：**預設勾選開啟惡意行為攔截。你也可以根據您的需要，對該預設項進行修改。

- ➢ 發現高威脅惡意行為，系統推薦將其清除。
- ➢ 發現一般惡意行為，系統推薦詢問用戶。

3.3.3 郵件監控

金山毒霸郵件監控運用全新的垃圾郵件過濾引擎，具有雙重過濾機制，雙向攔截郵件病毒，高效過濾垃圾郵件，讓您放心的收發電子郵件，遠離郵件病毒的侵擾。

啟動：

金山毒霸 V9.0 主介面"監控和防禦"頁面中選擇："郵件監控"→"詳細設定"；也可在"綜合設定"中選擇"防毒設定"→"郵件監控"，勾選"啟動郵件監控"。

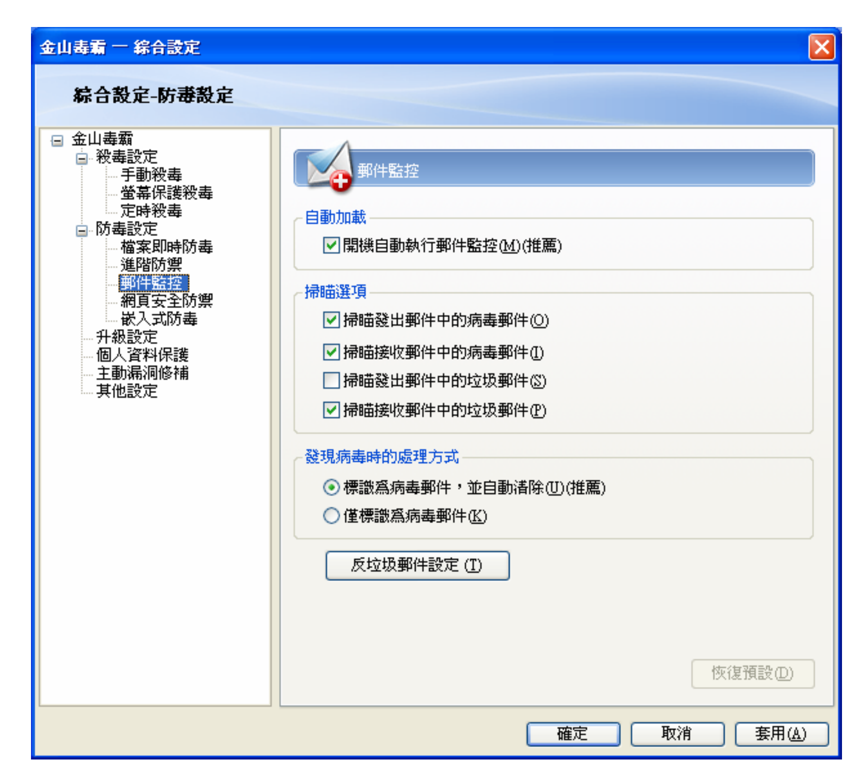
退出：

在主介面中選擇"監控和防禦"介面，然後選定"郵件監控"，點擊活動頁面中的"關閉"按鈕即可。

當您接收到垃圾郵件或病毒郵件時，在視窗右下角以氣泡窗口的形式彈出提示。

郵件監控綜合設定

首先切換到"監控和防禦"頁面，選擇"郵件監控"，再點擊"詳細設定"，然後於"防毒設定"中選定"郵件監控"。



各選項說明如下：

✓ **自動載入：**您在此可以設定開機自動運行郵件監控，設定後即允許金山毒霸隨系統啟動而開啟對郵件的即時監控，掃描收/發郵件中的病毒郵件和垃圾郵件，發現病毒自動清除，當清除失敗時將郵件中的病毒隔離，以免感染其他文件。清除失敗後處理方式請參見：**手動殺毒**。

✓ **掃描選項：**您在此可以設定需要掃描的郵件類型和範圍。

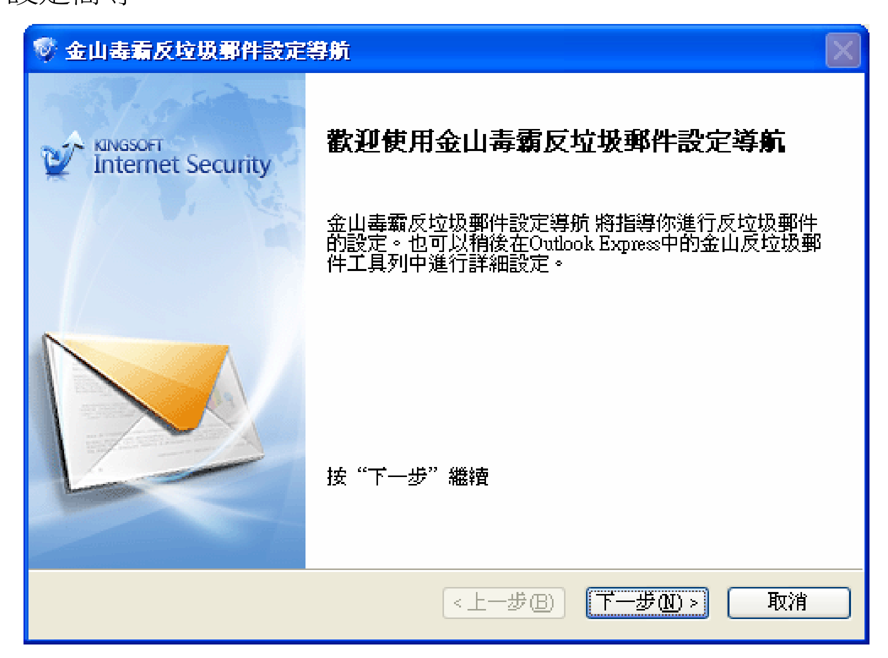
✓ **發現病毒時的處理方式**：對監控下發現的病毒的郵件，預設設定為“標識為病毒郵件，並自動清除”，您也可選擇“僅標識為病毒郵件”。

3.3.4 垃圾郵件過濾

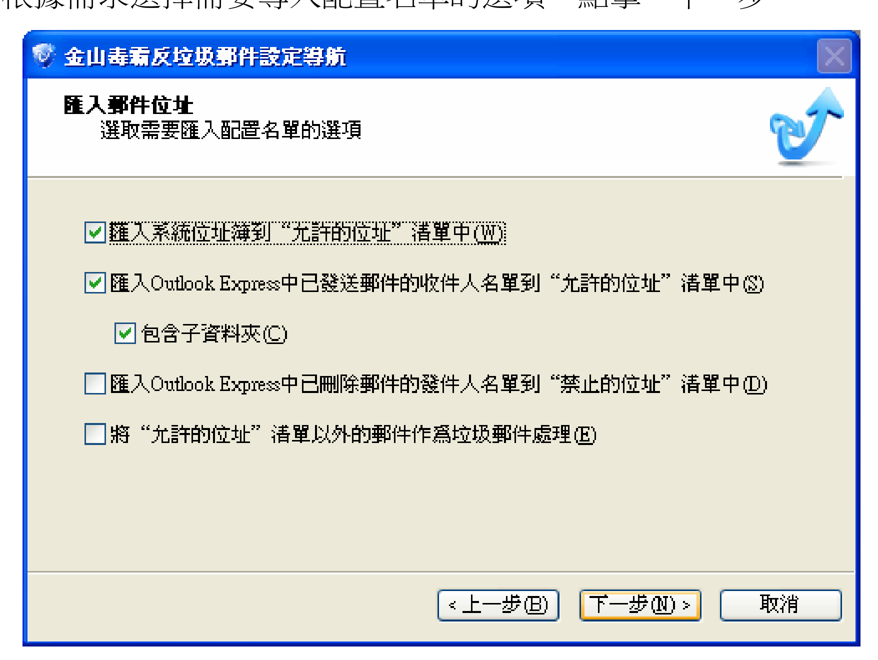
金山毒霸反垃圾郵件組件能夠和最常用的郵件用戶端之一：Outlook Express 6.0 緊密結合。當接收到垃圾郵件或病毒郵件時，金山毒霸反垃圾郵件元件能夠自動分類垃圾郵件和正常郵件以及自定義過濾選項。

安裝

當金山毒霸安裝完成後，首次開啟 Outlook Express6.0 程式時，自動進入金山毒霸反垃圾郵件設定嚮導。



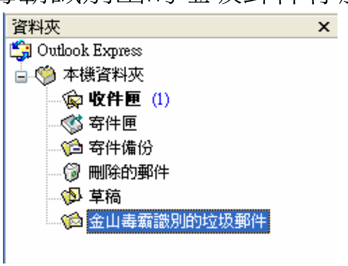
您可以根據需求選擇需要導入配置名單的選項，點擊“下一步”。



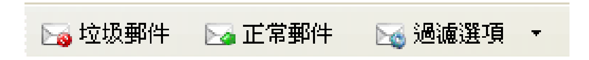
點擊“完成”，反垃圾郵件設定成功。您也可以在反垃圾郵件的功能表中選擇再次運行本嚮導。

使用方法

安裝完成後，打開的 Outlook Express 6.0 收件箱中會出現命名為“金山毒霸識別的垃圾郵件”的文件夾，被金山毒霸識別出的垃圾郵件存放於此。



同時，OE 介面上方會出現如下圖的按鈕：



✓ **垃圾郵件**：選中收件箱中的一封郵件，點擊“垃圾郵件”按鈕，則該郵件被轉移到“金山毒霸識別的垃圾郵件”文件夾中。

✓ **正常郵件**：選中“金山毒霸識別的垃圾郵件”文件夾中的一封郵件，點擊“正常郵件”按鈕，則該郵件被轉移到“收件箱”中。

✓ **過濾選項**：點擊“過濾選項”按鈕，進入金山反垃圾郵件設定。

➢ **常規**：當用戶的電腦中安裝 Oulook Express6.0 及以上版本時，自動啟動金山反垃圾郵件功能並預設啟動自動更新。凡垃圾郵件級別設定包括高、中、低三種等級，推薦設定為中等設定，即啟用允許、禁用列表，啟用啟發式識別掃描、關鍵字過濾及允許語言列表。

➢ **安全發件人**：在此用戶可自由添加允許接收郵件的發件人位址和功能變數名稱，並進行編輯或刪除；用戶還可以從位址簿或指定的檔夾的發件人或收件人地址導入安全發件人地址。

➢ **禁止地址列表**：在此用戶可自由添加認定是垃圾郵件的發件人位址和功能變數名稱，並進行編輯或刪除；用戶還可以從指定郵件檔夾發件人或收件人位址導入禁止的位址，並選擇當 OE 退出時清空金山反垃圾郵件文件夾。

➢ **關鍵字過濾**：用戶可在此設定允許或禁止的關鍵字，根據郵件中的標題和正文分別作自定義，來添加，編輯或刪除關鍵字列表項。

➢ **語言過濾**：用戶可根據郵件使用的語言進行垃圾郵件的設定，當接收到未被選中的語言的電子郵件將被作為垃圾郵件。

➢ **其他**：用戶可根據自己需求，進行其他處理選項及彈出視窗的設定，並設定埠。

➢ **備份和恢復**：用戶可在此備份和恢復所做的各種設定。點擊“過濾選項”旁的三角按鈕：

➢ **設定嚮導**：重新進行垃圾郵件過濾設定。

➢ **這是垃圾郵件**：選中用戶認定是垃圾郵件的郵件，點擊“這是垃圾郵件”，則該郵件轉移到“金山毒霸識別的垃圾郵件”文件夾中，並且該郵件位址將自動添

加到禁止的位址列表中。

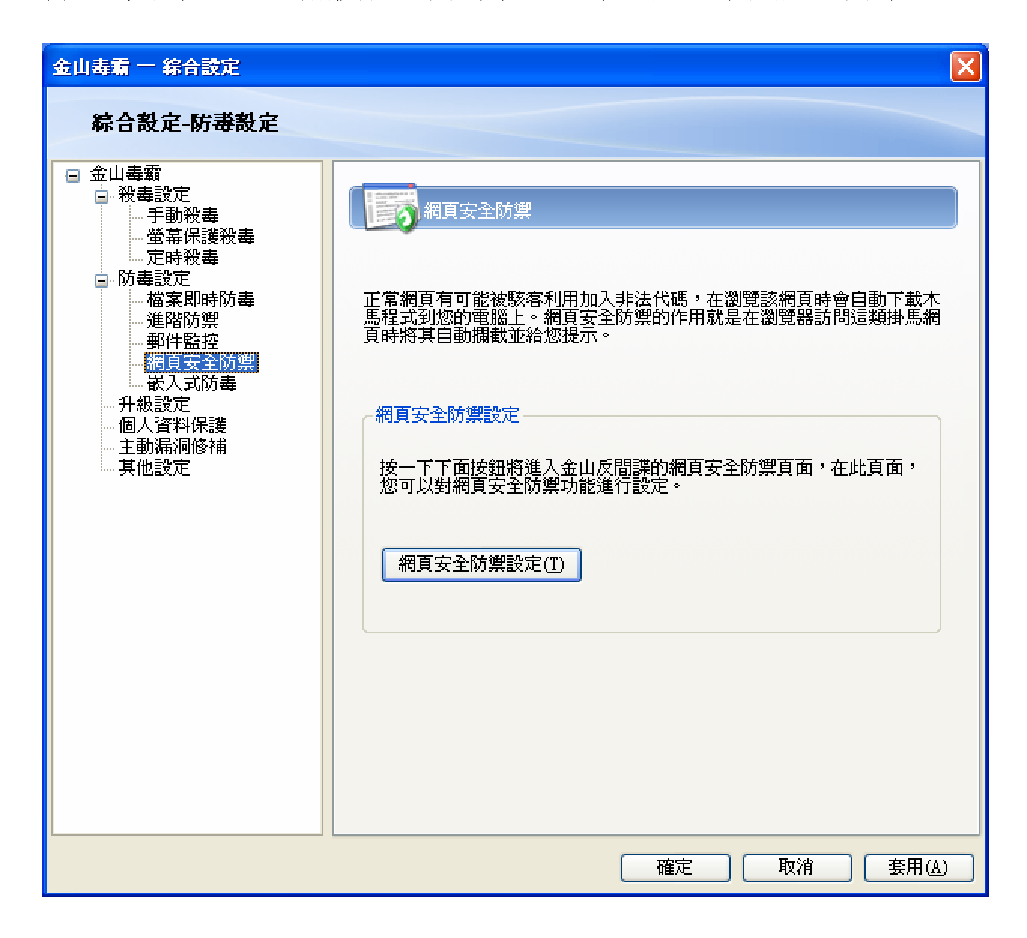
- **這不是垃圾郵件**：選中“金山毒霸識別的垃圾郵件”文件夾中的郵件，點擊“這不是垃圾郵件”，則該郵件被轉移到“收件夾”中，並且該郵件位址將自動添加到允許的位址列表中。
- **功能變數名稱禁止**：同上述“這是垃圾郵件”。
- **功能變數名稱許可**：同上述“這不是垃圾郵件”。
- **清空垃圾郵件文件夾**：點擊“清空垃圾郵件檔夾”，彈出是否確認的對話方塊，選擇“是”，則清空檔夾，選擇“否”，取消操作。
- **設定**：同上述金山反垃圾郵件設定。

3.3.5 網頁安全防禦

駭客利用對正常的網頁添加非法代碼，並利用 IE 漏洞在用戶不知情的情況下進行傳播。當您使用瀏覽器時訪問網頁時，瀏覽器便會自動下載木馬程式、病毒和其他惡意程式等到您的電腦上。金山毒霸的網頁安全防禦功能能有效地攔截並阻止該下載病毒和創建病毒進程的過程，保護您的瀏覽器的安全。

網頁安全防禦 **綜合設定**

首先切換到主介面中的“監控和防禦”頁面，於活動頁面中點擊“網頁安全防禦”，選擇“詳細設定”，然後於“防毒設定”中選定“網頁安全防禦”。



點擊介面中的“設定網頁安全防禦”按鈕，直接進入金山反間諜 V9.0 的網頁安全防禦頁面進行設定。

3.3.6 嵌入式防毒

金山毒霸智慧的嵌入 Office 套用程式和您所使用的聊天工具中，具有高度自動化和回應速度快等特點，防止病毒入侵，確保您工作和交流的安全。

3.3.6.1 Microsoft Office 嵌入式防毒

當您使用 Office 系列編輯文檔時，金山毒霸嵌入 Office 套用程式中，查殺巨集病毒程式並自動對打開的文檔進行病毒掃描，使您不必擔心所要編輯的檔已被病毒感染，是您值得信賴的 Office 安全助手，同時提醒您注意的是，本功能只支援 Microsoft Office 2000 以上的版本。

當您啟動辦公安全助手後，在使用辦公工具時，將自動嵌入到套用程式中的，對您處理的檔操作進行即時監控，一旦發現有消息感染病毒，第一時間通知您。

在此過程中，如果按 Esc 鍵、Enter 鍵，以及提示框右上角的關閉按鈕，預設您的選擇為跳過文件。

3.3.6.2 聊天工具嵌入防毒

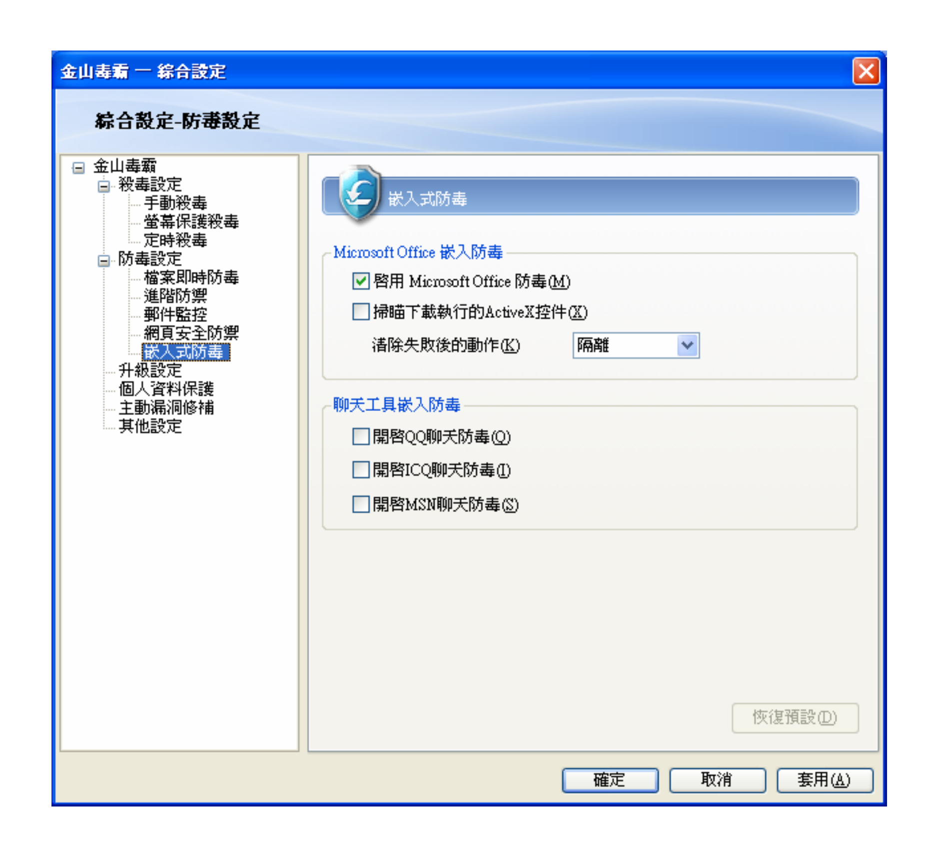
有調查數位顯示，QQ、ICQ、MSN 是目前互聯網下載及聊天的最主流軟體，由於使用 QQ、ICQ、MSN 而導致的密碼被盜、病毒侵襲、駭客攻擊也屢見不鮮，QQ、ICQ、MSN 安全助手以嵌入方式防護 QQ、ICQ、MSN 套用程式，結合金山毒霸引擎的強大功能，有效的遏制了不明來歷檔的攻擊，確保您網上交流的安全。

當您啟動聊天安全助手後，使用這些工具聊天時，將自動嵌入到聊天套用程式中的，對您收發的資訊進行雙向掃描，一旦發現有感染病毒消息，第一時間通知您。

當提示您發現病毒時，您可以根據自身需要選擇“清除病毒”、“刪除檔案”，“隔離檔案”、“跳過檔案”操作。

嵌入式防毒綜合設定

首先在功能表欄中選擇“工具|綜合設定”命令，然後在“防毒設定”中選定“嵌入式防毒”。



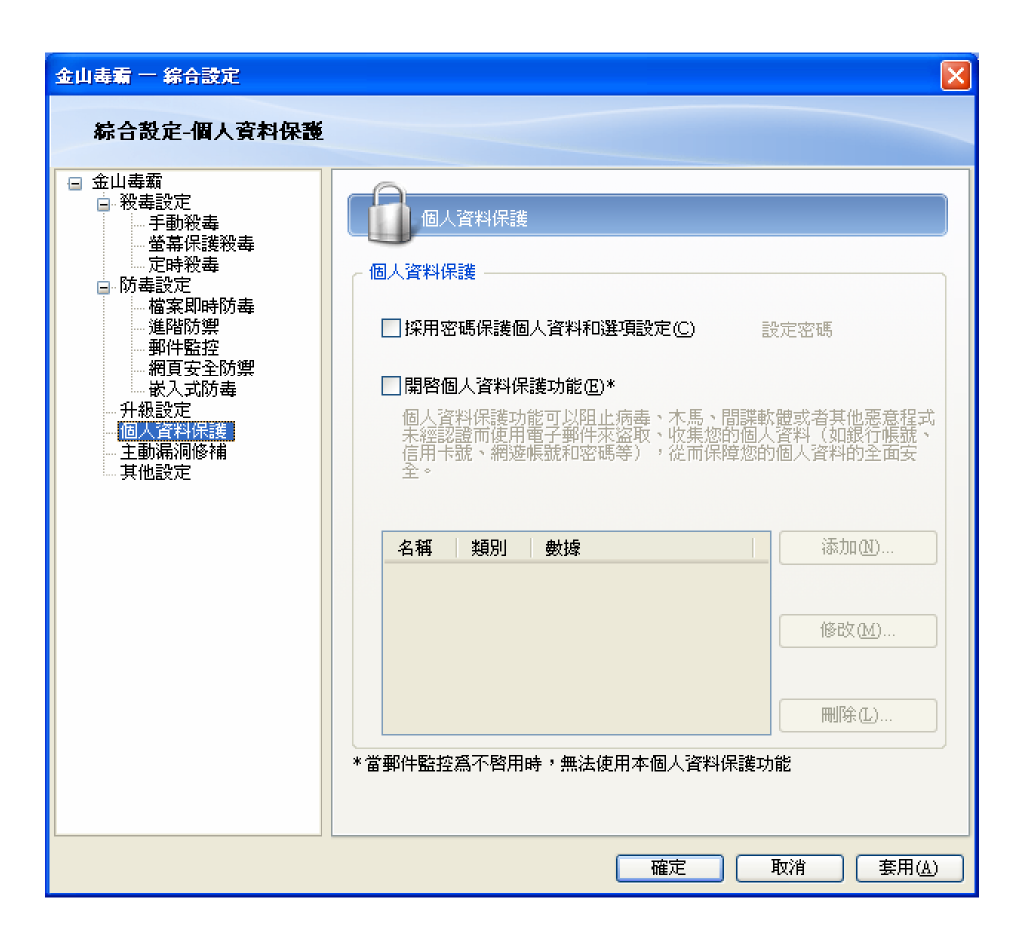
在 Microsoft Office 嵌入防毒中，您可以選擇啟動該防毒設定，以及掃描下載運行的 ActiveX 控制項。推薦發現病毒時自動清除，當清除失敗時將郵件隔離，以免感染其他文件。

在聊天工具嵌入防毒中，可開啟 QQ、ICQ 和 MSN 的聊天防毒。當您開啟相應的聊天工具時，嵌入防毒自動運行，保護套用程式的運行免受病毒侵襲。

3.3.7 個人資料保護

金山毒霸 V9.0 個人資料保護功能可以阻止病毒、木馬、間諜軟體或者其他惡意程式未經認證而使用電子郵件來盜取、收集您的隱私資料。它能幫助您加密保存您的密碼、電話號碼、銀行帳號及信用卡重要的資料，以保障資料的安全性。

首先在功能表欄中選擇“工具|綜合設定”命令，然後選定“個人資料保護”。



選中“採用個人資料和選項設定”，並設定密碼，設定完成後，以後每次設定個人資料保護選項時都需要輸入密碼。



選擇“開啟個人資料保護功能”，並于右邊單擊“添加”，在彈出的對話方塊中填入名稱、資料內容，並選擇類別，金山毒霸 V9.0　幫助您隱藏密碼、電話號碼、銀行帳號、信用卡號及其他資料資訊，您還可以修改及刪除這些資訊。

設定了個人資料保護的內容，當您發送郵件時，程式會自動監測，發現您的郵件中包含了您設定保護的內容後，彈出氣泡視窗提示您，由您決定是否繼續發送該郵件。

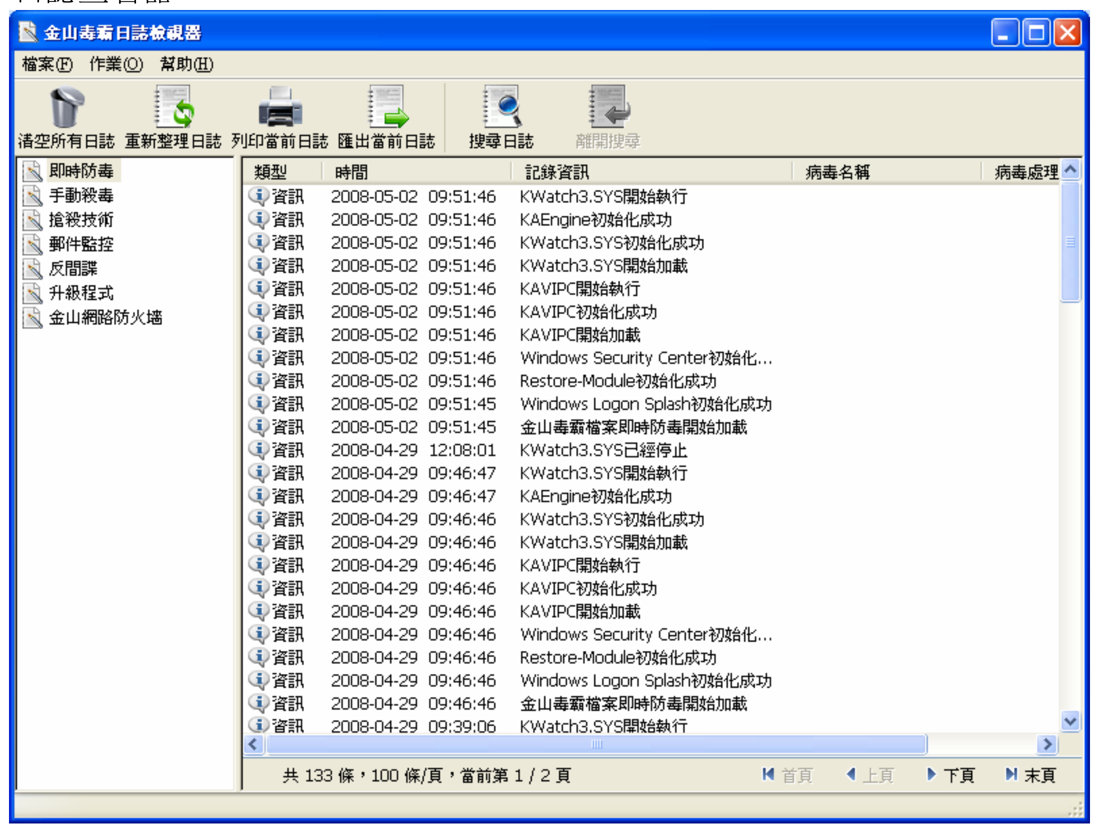
【注意】：確保郵件監控啟動時，才能使用個人資料保護功能。

3.4 工具篇

3.4.1 日誌查看器

金山毒霸的“日誌記錄”功能，準確的記錄了每一次查殺病毒操作的詳細情況，包括查毒時間、查毒類型、記錄資訊、病毒名稱和處理方式等資訊。該版本的日誌進一步細化，分為檔即時防毒日誌、手動殺毒日誌、搶先殺毒日誌、郵件監控日誌、反間諜日誌、升級程式日誌和金山網路防火牆日誌。

通過“開始”|“所有程式”|“金山毒霸 V9.0 網路安全套裝 ”|“金山毒霸工具”|“日誌查看器”，或者於主程序介面的功能表欄中選擇“工具”，在彈出的下拉功能表中選定“日誌查看器”。



✓ 即時防毒

檔案即時防毒的啟動、退出以及發現病毒，對病毒的處理方式等情況均在此有記錄。

✓ 手動殺毒

主程序每次查殺病毒後自動生成日誌，準確記錄查殺病毒操作的詳細情況，包括查毒任務的描述、查毒結果以及其資料統計（掃描檔數、總掃描時間、染毒檔數）資訊。

- ✓ **搶先殺毒**
  搶先殺毒的運行以及殺毒情況均在此有記錄。
- ✓ **郵件監控**
  郵件監控的啟動、退出以及處理垃圾郵件的情況均在此有記錄。
- ✓ **金山反間諜**
  金山反間諜的啟動、退出以及查殺惡意軟體的情況均在此有記錄。
- ✓ **升級程式**
  升級程式的啟動、完成、具體的更新時間均在此有記錄。
- ✓ **金山網路防火牆**
  金山網路防火牆的啟動、退出均在此有記錄。

3.4.2 創建應急隨身碟

當您的 Windows 系統被病毒感染，完全癱瘓不能啟動時，當您電腦系統檔被破壞或刪除時，當您需要修復硬碟分區表資訊時，您都離不開應急隨身碟。隨身碟盤可以幫助您進入一個安全無毒的環境，進行殺毒。

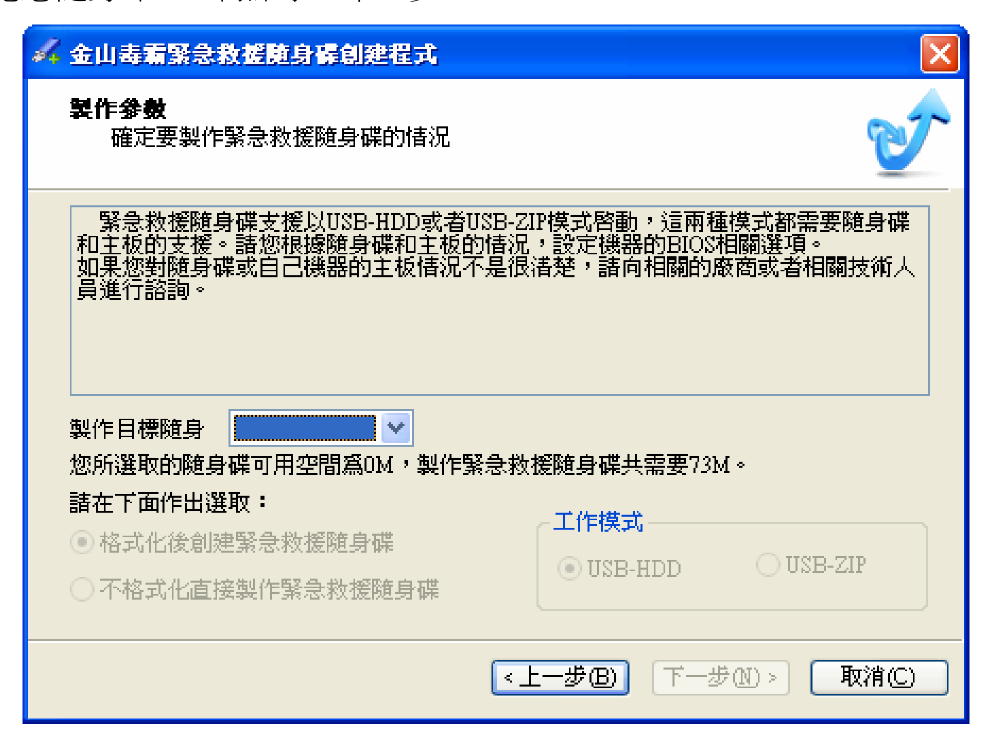
首次製作金山毒霸應急隨身碟步驟

【注意】：請先確認您的主板以及隨身碟所支援的隨身碟啟動方式，並且備份隨身碟內的資料。

通過“開始”|“所有程式”|“金山毒霸 V9.0 網路安全套裝 ”|“金山毒霸工具”|“創建應急隨身碟” ，或者通過金山毒霸主介面功能表欄中“工具”→“創建應急隨身碟” 。



✓ 選擇已閱讀“金山毒霸應急隨身碟製作聲明”，點擊“下一步”，按照您的主版和隨身碟所支援的啟動模式，選擇工作模式（USB-HDD 或 USB-ZIP），並選擇“格式化後創建應急隨身碟”，再點擊“下一步”。



✓ 彈出提示框，若您確認隨身碟中無數據或已做重要資料備份，請點“確定”繼續下面的操作。

✓ 接著進行隨身碟的啟動部分資料的製作。

✓ 隨身碟啟動部分的資料製作完畢，彈出提醒對話方塊，請您按提示拔出隨身碟後，再重新插入隨身碟，再點“下一步”。

✓ 應急殺毒部分的資料製作完畢後，會顯示應急隨身碟製作完成的介面，點擊“完成”，即成功製作了一張殺毒應急隨身碟。

【注意】在首次製作金山毒霸應急隨身碟時，您需要製作啟動部分和殺毒部分的資料，而以後每次製作時，無需製作啟動部分的資料。

非首次製作金山毒霸應急隨身碟步驟：

✓ 通過“開始”|“所有程式”|“金山毒霸 V9.0 網路安全套裝”|“金山毒霸工具”|“創建應急盤”，或者通過金山毒霸主介面功能表欄中“工具”→“創建應急盤”。

✓ 點擊“下一步”，按照您的主板和隨身碟所支援的啟動模式，選擇工作模式（USB-HDD 或 USB-ZIP），並選擇“不格式化直接製作應急隨身碟”，再點擊“下一步”。

✓ 彈出提示框，若您確認隨身碟中無數據或已做重要資料備份，請點“確定”繼續下面的操作。

✓ 接著直接跳過隨身碟啟動部分的資料製作過程，進行應急殺毒部分資料製作，顯示如下：

✓ 應急殺毒部分的資料製作完畢後，會顯示應急隨身碟製作完成的介面，點擊“完成”，即成功製作了一張殺毒應急隨身碟。

✓ 使用金山毒霸應急隨身碟
✓ 請您根據隨身碟和主板的情況，設定機器的 BIOS 相關選項。如果您對隨身碟或者電腦的主板情況不清楚，請向相關的廠商或者相關技術人員進行諮詢。
✓ 請插入創建好的應急隨身碟。
✓ 重啟電腦，重啟完成後，應急隨身碟將自動對您的電腦進行全面查毒。

3.4.3 病毒隔離系統

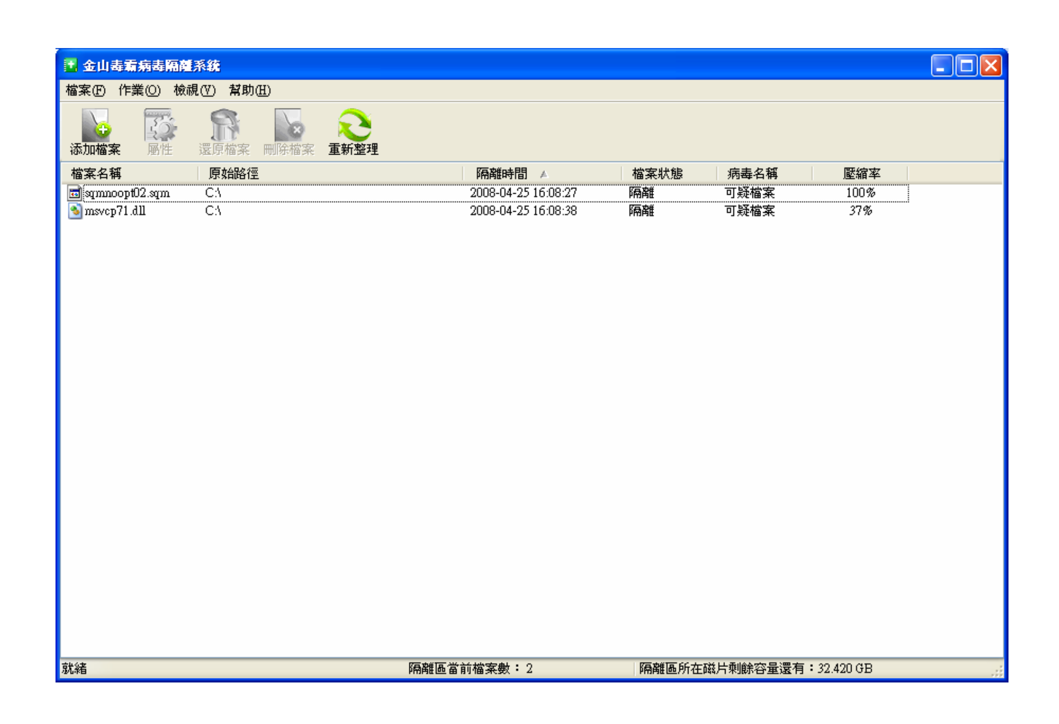
金山毒霸病毒隔離系統幫您隔離以下三類檔，讓您電腦免受潛在病毒威脅。

✓ 套用於殺毒軟體過程中，可以發現病毒，但不能殺染毒檔；
✓ 感染未知病毒檔；
✓ 用戶懷疑但不能確定是否含有病毒的可疑檔。

通過“開始”|“所有程式”|“金山毒霸 V9.0 網路安全套裝”|“金山毒霸工具”|“病毒隔離系統”或者在金山毒霸主介面選擇“工具”→“病毒隔離系統”即可啟動該項工具。

功能簡介

✓ **添加檔案**：將需要隔離的檔案添至隔離系統；
✓ **屬性**：查看所隔離檔屬性；
✓ **還原檔案**：恢復隔離檔案到原有目錄；
✓ **刪除檔案**：將染毒檔案從磁片上徹底刪除；
✓ **重新整理**：刷新隔離檔案目錄列表；
✓ **排列圖示**：對隔離區所有檔按檔案名稱、原始路徑、隔離日期、檔狀態、病毒名稱、壓縮比率進行排序，檔以大圖示、小圖示、列表、詳細資料形式陳列。



【注意】：雙擊或右鍵單擊被隔離的文件，彈出有關該檔屬性的對話方塊以及金山毒霸對您提出的建議。病毒隔離區的最大容量是 128M，當檔案超過 128M 時，隔離時間最長的檔將自動被刪除。

3.4.4 可疑檔掃描

金山毒霸的“可疑檔掃描”功能，將幫助您搜索電腦中可能成為病毒的可疑程式，並記錄該可疑程式的詳細情況，包括檔案名、檔大小、時間日期、存在路徑及存在的原因。

通過主介面的功能表欄中選擇“工具”，在彈出的下拉功能表中選定“可疑檔案掃描”即可。單擊“開始掃描”，掃描開始，在掃描進度中顯示掃描的路徑，完成後顯示掃描到的可疑檔案的詳細資訊。



單擊“立即上報”，彈出選擇上報方式的對話方塊，系統推薦通過網路將可疑檔案直接上報給金山軟體有限公司，您也可選擇先保存到磁片中，以後通過其他途徑提供給金山軟體有限公司。

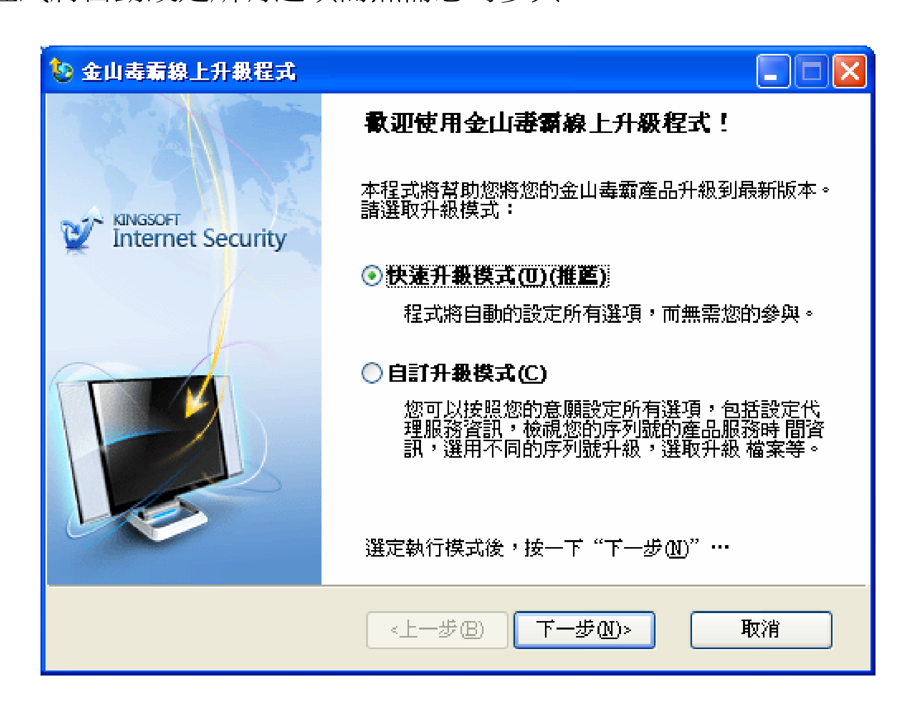
3.5 升級篇

金山毒霸 V9.0 改變了安全軟體的升級服務模式。一旦重大病毒爆發，在新的病毒特徵庫更新到伺服器後，所有安裝金山毒霸 V9.0 的線上用戶電腦會被通知在 30 分鐘內甚至更短的時間內自動連接伺服器進行升級，確保用戶及時獲得最新的病毒特徵庫，防範最新爆發的病毒，確保電腦的安全。

大部分情況下升級過程無需您的干預，在您的電腦連接到互聯網的時候，自動即時升級將會自動幫助您將病毒庫即時更新。同時也提供了手動升級的途徑，使您獲得最良好的軟體升級體驗。金山毒霸 V9.0 可以通過 Internet、以增量方式更新病毒庫和查毒引擎，更新過程無需用戶過多的操作，為您節省寶貴時間。智慧升級程式使用簡單、介面友好、支援中斷點續傳、使您的升級過程有質的飛躍。

3.5.1 快速升級

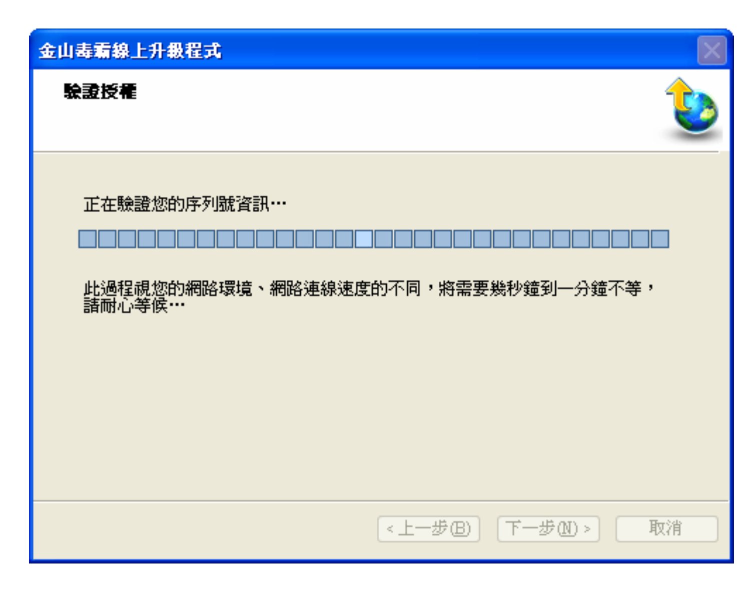
單擊毒霸主介面的“線上升級”或選擇“工具”→“線上升級”，都可以啟動線上升級的程式。在運行模式中選擇快速升級模式或自定義升級模式。若您選擇了快速升級模式，則程式將自動設定所有選項而無需您的參與。



單擊“下一步”，下載並分析升級資訊後，進入金山序列號的驗證頁面。如果您在安裝時未輸入金山毒霸用戶服務卡上的金山序列號及如果您不知道金山序列號的所在位置，您可以通過此對話方塊的提示。



在金山毒霸 V9.0 網路安全套裝中尋找序列號碼，輸入相關資訊後點擊“下一步”進行驗證。



開始下載升級。在對話方塊中顯示下載並分析升級資訊的進度以及驗證用戶資訊的合法性，當下載進度條達到 100%時，升級檔下載完成；

單擊下一步，點擊“完成”，恭喜您已順利完成整個升級過程！您可以查看“升級報告”並保存。

如果有最新的漏洞庫檔更新，升級完成後的對話方塊將提示您選擇立即進行漏洞修復。

此時金山毒霸 V9.0 預設勾選“現在就進行漏洞修復”，點擊“完成”，則立即進行漏洞掃描。

3.5.2 自定義升級

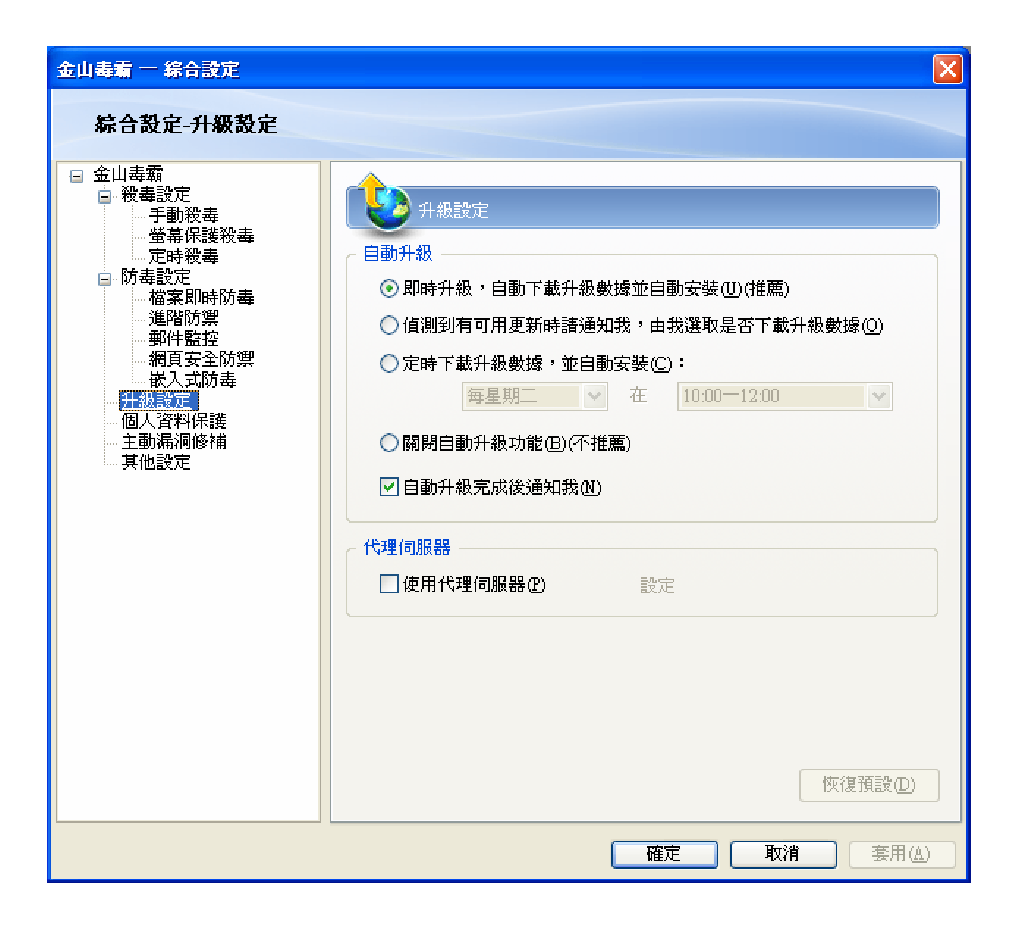
在“運行模式”中，您也可以選擇“自定義升級模式”。單擊“下一步”，在出現的升級方式中選擇“從 Internet 上升級”。

3.5.2.1 從 Internet 上升級

若您選擇了“從 Internet 上升級”，點擊“下一步”，下載並分析升級資訊，進入金山序列號的驗證頁面。餘下步驟請參見“快速升級”中的相關內容。

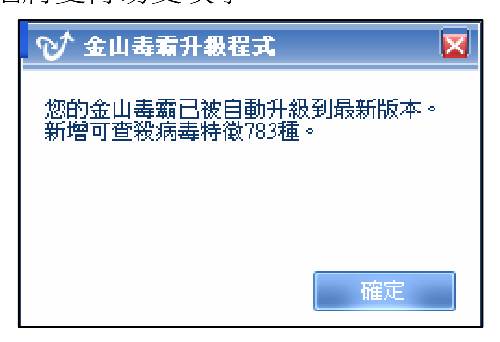
3.5.3 升級設定

首先切換到活動標籤中的“監控和防禦”頁面，於活動頁面中點擊“服務|主動即時升級”→“詳細設定”。



各項說明如下：

✓ **自動升級**：系統推薦即時升級，自動下載升級資料並自動安裝；您也可根據需要設定檢測到有可用更新時請通知我，由我選擇是否下載升級資料；或者還可以定時下載升級資料，並自動安裝；系統不推薦關閉自動升級功能，因為如果您不按期下載病毒庫更新，您的電腦將變得易受攻擊。



✓ **代理伺服器**：當您使用代理伺服器時，選中對應項，對代理伺服器進行設定。預設直接使用 IE 瀏覽器中的代理伺服器設定升級，當使用特定的代理伺服器時，選定“自定義代理伺服器設定”，然後選定伺服器類型：HTTP、Socket5 代理；填寫伺服器位址、埠；同時請輸入登錄時的用戶名、密碼（當代理伺服器需要填寫時）。

第四章 金山網路防火牆 V9.0

4.1 入門篇

4.1.1 產品特色

金山網路防火牆 V9.0 是一款功能強大、方便易用的個人及家庭首選網路防火牆產品之一。它能保護您的電腦免受病毒、駭客、垃圾郵件、木馬和間諜軟體等網路危害。

網路個人防火牆

提供對駭客程式、木馬和間諜軟體以及其他惡意程式的攔截查殺，對網路進行全方位的防護，同時提供了網路訪問監控、共用目錄管理、不良網站過濾等多種網路安全實用功能。

木馬防火牆

通過多種技術，實現對木馬進程的查殺。系統中一旦有木馬、駭客或間諜程式訪問網路，木馬防火牆會及時攔截該程式對外的通信訪問，然後對記憶體中的進程進行自動查殺，保護用戶網路通信的安全。所以，木馬防火牆對防禦盜取用戶資訊的木馬、駭客程式特別有效。

網路狀態監控

全面提供當前活動網路狀態的詳細資訊，並可進一步採取打開該程式目錄，或終止該程式的操作，杜絕一切惡意程式企圖侵害您的電腦。

自定義IP規則設定

強大的自定義 IP 規則編輯器，讓熟悉網路協定的您，可對互聯網和局域網上的資料埠進行相應的調配，進一步規範您的電腦運作，避免因來自任何不同地方的惡意攻擊而為您造成損失。

4.1.2 主介面介紹

訪問金山網路防火牆 V9.0，請執行下列任一操作：

✓ 在桌面雙擊“金山網路防火牆”圖示。



✓ 在 Windows 任務欄中狀態欄雙擊金山網路防火牆的小圖示“ ”或右鍵單擊該圖示，在彈出的功能表中選擇“打開金山網路防火牆”。

✓ 在 Windows 2000 任務欄中，單擊“開始→程式→金山毒霸 V9.0 網路安全套裝→金山網路防火牆 V9.0”。

✓ 在 Windows XP 任務欄中，單擊開始→所有程式→金山毒霸 V9.0 網路安全套裝→金山網路防火牆 V9.0。

✓ 在 Windows Vista 任務欄中，單擊開始→程式→金山毒霸 V9.0 網路安全套裝→金山網路防火牆 V9.0。



✓ **菜單欄**：採用Windows標準風格，單擊其中任何一項功能表，即可彈出詳細的下拉功能表，您可以方便、快捷地選定您所需的功能功能表。

✓ **標籤欄**：包括四個活動標籤“安全狀態”、“監控狀態”、“套用規則”和“網路狀態”。預設啟動“安全狀態”，您可以根據自身需要切換活動標籤，同一時間有且只有一個活動標籤。

- **安全狀態**：當前網路活動狀態、網路活動日誌、用戶目前網路安全狀態。
- **監控狀態**： 包括互聯網監控和局域網監控，用戶可在此頁面調整網路安全級別，預設安全級別為“中”。
- **套用規則**：用戶可在此查看電腦中曾經運行過的套用程式許可權規則的詳細資訊及用戶的設定。
- **網路狀態**：顯示用戶電腦的網路連接狀態的詳細資訊。

✓ **活動頁面**：隨標籤的變化而不時更換的模組則為活動頁面，它是金山網路防火牆最常用功能操作平臺，在頁面中可以進行各項功能的細則操作和設定。

4.2 使用篇

4.2.1 快速使用

4.2.1.1 啟動金山網路防火牆 V9.0

電腦安裝金山毒霸 V9.0 網路安全套裝之後，金山網路防火牆 V9.0 會自動啟用，保護您的電腦，幾乎不需要您更改任何設定。您還可以通過以下步驟啟用並確保金山網路防火牆 V9.0 處於正常的工作狀態。

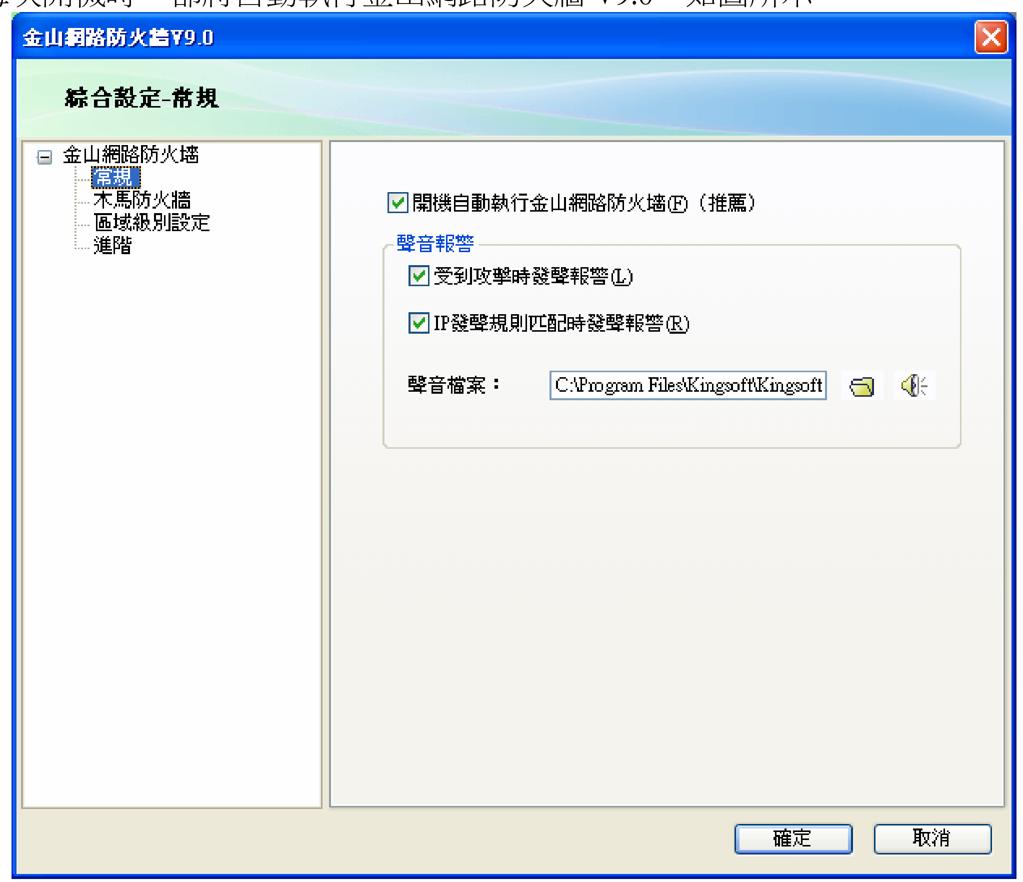
確保啟用金山網路防火牆V9.0，

查看 Windows 任務欄（包含“開始”按鈕，預設情況下顯示在桌面底部的工具欄）中狀態欄是否出現金山網路防火牆 V9.0 的小圖示“”，如果可以看到，說明您的電腦系統一直處於金山網路防火牆 V9.0 的監控保護下。

4.2.1.2 開機自動執行

如果每次系統啟動後，金山網路防火牆 V9.0 不能自動啟動。這時，就需要對金山網路防火牆 V9.0 的配置選項進行更改：

- ✓ 打開金山網路防火牆 V9.0 的主介面。
- ✓ 單擊“功能表欄”中“工具”→“綜合設定”，選擇“常規”。
- ✓ 用滑鼠單擊“開機自動執行網路防火牆”此選項前的選擇框，將出現“√”，表示您在每次開機時，都將自動執行金山網路防火牆 V9.0，如圖所示：



您也可以通過以下任意一種方法實現開機自動執行金山網路防火牆：

✓ 右擊 Windows 任務欄（包含“開始”按鈕，預設情況下顯示在桌面底部的工具欄）中狀態欄“ ”選中“開機自動執行”。

✓ 單擊金山網路防火牆 V9.0 主介面功能表欄中的“操作”→“開機自動執行

4.2.1.3 斷開網路

在金山網路防火牆 V9.0 主介面中，您可以看到“斷開網路”按鈕。如圖紅色區域所示：



單擊此按鈕，金山網路防火牆V9.0 將終止電腦和網路之間的連接，限制以下情況對電腦的破壞：受到攻擊、特洛伊木馬、未經允許發送個人資訊，或者不小心允許不可信任的人訪問電腦上的檔。總之，杜絕任何可能的駭客攻擊。

在解決安全問題時斷開網路避免受到攻擊

✓ 打開金山網路防火牆 V9.0 的主介面。

✓ 在金山網路防火牆 V9.0 主介面下方，單擊“斷開網路”按鈕，這時您可以看到該按鈕上的“斷開網路”字樣變成了“恢復網路”，此時，Windows 系統中的金山網路防火牆小圖示“ ”變為“ ”

✓ 此時，您的電腦與網路和其他電腦之間的任何通信都已經中止。“斷開網路”是解決安全問題的臨時方法，只要單擊“恢復網路”按鈕，金山網路防火牆 V9.0 就會重新允許所有的傳入和傳出通信。

4.2.1.4 使用 Windows 任務欄中的金山網路防火牆圖示

當用戶的電腦安裝了金山網路防火牆 V9.0 後，系統託盤中會自動添加金山網路防火牆的小圖示“ ”右鍵單擊該圖示，可以進行如下操作：

- ✓ 打開金山網路防火牆
- ✓ 進行線上升級操作
- ✓ 斷開或恢復網路連接
- ✓ 設定開機時自動運行金山網路防火牆
- ✓ 退出金山網路防火牆

4.2.1.5 線上升級

金山網路防火牆 V9.0 是依賴當前資訊來防止電腦受到新的安全威脅。通過線上升級可以給您的金山網路防火牆 V9.0 提供最新資訊，將程式更新和防護更新下載到您的電腦。您可以通過以下任何一種方法打開金山網路防火牆線上升級程式：

- ✓ 單擊金山網路防火牆 V9.0 主介面功能表欄中的“工具”→“線上升級”。
- ✓ 右擊 Windows 任務欄（包含“開始”按鈕，預設情況下顯示在桌面底部的工具欄）中狀態欄“ ”選中“線上升級”。

金山毒霸 V9.0 網路安全套裝中毒霸和網路防火牆的升級是統一的升級，即毒霸升級後網路防火牆會同步被升級，同樣網路防火牆升級後毒霸也同步被升級。網路防火牆的所有升級過程及操作同毒霸一樣。（詳見毒霸升級篇內容）

4.2.2 查看當前狀態

查看當前狀態包括查看金山網路防火牆 V9.0 的元件資訊及系統安全狀態，如何確保升級及即時防毒已經開啟。

4.2.2.1 查看元件資訊

在金山網路防火牆 V9.0 主介面功能表欄點擊“幫助”→“關於金山網路防火牆 V9.0”，可以查看元件資訊。內容包括：

- ✓ 金山網路防火牆 V9.0 程式版本
- ✓ 木馬庫版本
- ✓ 許可協議
- ✓ 客服資訊及毒霸資訊安全網的鏈結

4.2.2.2 查看系統安全狀態

將主介面切換至“安全狀態”頁面，便可查看系統安全狀態：



當前網路活動狀態。

該區域右邊有三個圖示分別表示：

跳轉到詳細資訊：點擊該圖示，可直接跳轉到網路狀態下，詳細列出網路的活動狀態。

打開程式所在檔夾：選擇一個程式再點擊該圖示，您就可以清楚地瞭解該程式在哪個檔夾下。

關閉程式：選擇一個程式再點擊該圖示，就可以結束一個不必要的程式。

網路活動日誌。

該區域可以直觀地記錄您電腦中網路活動的狀況。

如果您懷疑當前網路活動不太正常，可直接點擊“斷開網路”，終止用戶的電腦和網路之間的連接，杜絕任何可能的駭客攻擊。

如果需要連接網路，可直接點擊“恢復網路”，則電腦和網路之間已連接，你的電腦正處於金山網路防火牆的安全保護之下。

4.2.3 網路監控狀態

在金山網路防火牆 V9.0 的“監控狀態”頁面可顯示互聯網監控狀態和局域網監控狀態。用戶可以設定互聯網和局域網的安全級別（預設安全級別為中），還可以自定義 IP 規則，可以自主的添加、修改、刪除一些 IP 規則。

4.2.3.1 安全級別設定

金山網路防火牆 V9.0 為您提供互聯網和局域網的防火牆策略的安全級別設定功能，您可以通過滑杆的滑動來選擇適合高、中、低的安全級別。如圖所示：



- ✓ 高安全級別
  對訪問網路的套用程式進行許可權控制；
  對常見的木馬和駭客攻擊進行攔截；
  提供嚴格控制的網路訪問許可權，禁止別人探測、訪問本機。
- ✓ 中安全級別（預設）
  對訪問網路的套用程式進行許可權控制；
  對常見的木馬和駭客攻擊進行攔截；
  提供用戶日常適用的網路訪問許可權，例如瀏覽網頁、收發郵件等。
- ✓ 低安全級別
  對訪問網路的套用程式進行許可權控制；
  對常見的木馬和駭客攻擊進行攔截；
  提供寬鬆自由的網路訪問許可權。

4.2.3.2 自定義 IP 規則

除了系統提供的高、中、低三種預設安全級別外，用戶還可以自定義安全級別。熟悉網路協定的用戶可以自主的添加、修改、刪除 IP 規則，也可以對所有的編輯條目做保存和清空的選擇並根據用戶的需要設定 IP 規則優先順序。

用戶可以通過點擊金山網路防火牆 V9.0 主介面的“監控狀態”在彈出的頁面右側點擊“詳細設定”，打開“自定義 IP 規則編輯器”如圖所示：

自訂 IP 規則編輯器

添加 修改 刪除 向上移動 向下移動 保存 清空 匯入 匯出

規則名稱	動作	協定	方向	對方 IP 位址	本機數據連...	對方數據連...
允許別人使用 Ping 命令探測本機	允許	ICMP	接收	任何位址		
允許自己用 Ping 命令探測其他...	允許	ICMP	接收	任何位址		
允許本機接收"超時"的 ICMP 回...	允許	ICMP	接收	任何位址		
允許本機接收"無法到達"的 ICM...	允許	ICMP	接收	任何位址		
防止 ICMP 類型攻擊	攔截	ICMP	接收	任何位址		
防止 IGMP 類型攻擊	攔截	IGMP	接收	任何位址		
允許功能變數名稱 DNS 解析（U...	允許	UDP	接收	任何位址	任何連接埠	53
允許別人探測本機的機器名稱（...	允許	UDP	收/發	任何位址	134 - 139	任何連接埠
允許別人訪問本機的共用資源（...	允許	TCP	收/發	任何位址	134 - 139	任何連接埠
允許別人訪問本機共用資源(Win...	允許	TCP	收/發	任何位址	445	任何連接埠
允許自己探測他人的機器名稱（...	允許	UDP	收/發	任何位址	任何連接埠	134 - 139
允許自己訪問他人的共用資源（...	允許	TCP	收/發	任何位址	任何連接埠	134 - 139
允許自己訪問他人共用資源(Win...	允許	TCP	收/發	任何位址	任何連接埠	445
允許別人與本機的缺省 Web 網...	允許	TCP	收/發	任何位址	80 - 83	任何連接埠
允許別人與本機的 Web 網頁服...	允許	TCP	收/發	任何位址	8080	任何連接埠
允許別人與本機的缺省 HTTPS ...	允許	TCP	收/發	任何位址	443	任何連接埠
允許別人與本機的缺省 POP3 郵...	允許	TCP	收/發	任何位址	110	任何連接埠
允許別人與本機的缺省 SMTP 郵...	允許	TCP	收/發	任何位址	25	任何連接埠
允許別人與本機的缺省 FTP 網路...	允許	TCP	收/發	任何位址	20 - 21	任何連接埠
允許訪問外部 HTTP 資源（流覽...	允許	TCP	收/發	任何位址	任何連接埠	80 - 83
允許訪問外部 HTTP 資源（流覽...	允許	TCP	收/發	任何位址	任何連接埠	8080

允許別人發送給本機的類型為 8 的 ICMP 數據包，從而他人可以使用 Ping 命令探測本機是否存在於網路中

在 IP 規則編輯器中可以對 IP 規則進行下列操作：

✓ 添加新的 IP 規則

單擊“添加”按鈕，在彈出的“添加 IP 資料包過濾規則”視窗中可以設定規則名稱、規則描述、對方的 IP 位址、資料傳輸方向、資料協定類型、本地埠、對方埠、TCP 標誌以及滿足上述條件時的動作。

✓ 修改現存的 IP 規則

在已定義的 IP 規則列表中，選中要修改的 IP 規則，單擊“修改”按鈕，在彈出的“修改 IP 資料包過濾規則”視窗中進行相應的修改，包括規則名稱、規則描述、對方的 IP 位址、資料傳輸方向、資料協定類型、ICMP 資料包匹配條件以及滿足上述條件時的動作。

✓ 刪除現存的 IP 規則

在已定義的 IP 規則列表中，選中要刪除的 IP 規則，點擊“刪除”按鈕。在彈出的“警告”視窗中，點擊“確定”按鈕將繼續該操作，刪除選中的 IP 規則；點擊“取消”按鈕則將撤銷刪除動作。

✓ 啟用或禁用

用滑鼠單擊規則名稱前的選擇框，將出現“√”，表示啟用此項 IP 規則。否則，表示該 IP 規則處於禁用狀態。

✓ 調整 IP 規則優先順序

單擊“向上移動”按鈕將提高被選中的 IP 規則的優先順序，單擊“向下移動”按鈕將降低被選中的 IP 規則的優先順序。

✓ 保存和清空

當您完成對 IP 規則的編輯時，單擊“保存”按鈕，並在彈出的窗口中點擊“確定”按鈕，在金山網路防火牆 V9.0 的主介面中的網路安全級別中選擇“自定義級別”，即可套用此設定。當您需要清除 IP 規則列表中的所有 IP 規則，單擊“清空”按鈕，即可刪除當前 IP 規則列表中的所有 IP 規則。

✓ 匯入或匯出

單擊“匯入”按鈕，則可以導入對應防火牆產品的 IP 資料包過濾規則。 單擊“匯出”按鈕，將當前的 IP 規則列表存成新的金山網路防火牆自定義 IP 規則，預設規則的檔類型為（*.dat）。

4.2.4 套用程式規則

金山網路防火牆 V9.0 增加了對套用程式資料包進行底層分析攔截的功能，它可以控制套用程式發送和接收資料包的類型、通訊埠，並且決定攔截還是通過，這是目前其他很多軟體防火牆不具有的功能。在啟動金山網路防火牆 V9.0 的情況下，任何套用程式只要有通訊資料包發送和接收存在，這些都會先被金山網路防火牆 V9.0 首先截獲分析。

當套用程式提出訪問網路的請求時，金山網路防火牆 V9.0 會彈出詢問視窗，且將操作結果自動加入“套用規則”的列表中。列表顯示所有已啟動套用程式的詳細資訊，包括開始運行時間以及所在路徑。在該套用程式旁邊還有“允許”、“禁止”、“詢問”三個選項，分別表示目前金山網路防火牆 V9.0 對該程式提出訪問網路請求時所採取的操作——允許該程式訪問網路、禁止該程式訪問網路以及當該程式訪問網路時向用戶詢問是否允許。

用戶可以根據需要添加或刪除“套用規則”列表中的套用程式網路訪問許可權規則。

4.2.4.1 彈出的氣泡窗口

金山網路防火牆 V9.0 啟動後，如果電腦中的套用程式對網路進行訪問，金山網路防火牆就會彈出視窗，詢問您是否允許該程式訪問網路。



你可以進行如下操作：

✓ 對於每次使用都需要訪問網路的套用程式，您可以勾選“總是允許”。

✓ 對於不是每次使用都需要訪問網路的套用程式，您可以根據實際情況選擇“本次允許”或“本次禁止”。

✓ 對於要訪問網路的可疑套用程式，您可以勾選“總是禁止”。

4.2.4.2 查看套用程式許可權

當套用程式提出訪問網路的請求時，金山網路防火牆 V9.0 會彈出詢問視窗，且將操作結果自動加入“套用規則”的列表中。列表顯示出所有已啟動套用程式的詳細資訊，包括開始運行的時間以及程式所在地址。

打開金山網路防火牆 V9.0 的主介面。在金山網路防火牆 V9.0 主介面中，單擊“套用規則”標籤。在“套用規則”視窗列表中，可以查看到曾經提出訪問網路請求的套用程式的版本、名稱、開始運行時間、大小及安裝路徑等詳細資訊。也可以看到當前金山網路防火牆 V9.0 對該程式提出訪問網路請求時所採取的操作，如圖所示：



4.2.4.3 更改套用程式規則

在該套用程式欄右邊有“允許”、“禁止”、“詢問”三個選項，分別表示該程式提出訪問局域網、互聯網和發出郵件請求時金山網路防火牆 V9.0 所採取的操作：

✓ 允許該程式訪問網路。

✓ 禁止該程式訪問網路。

✓ 該程式訪問網路時，網路防火牆會彈出視窗詢問用戶是否允許該程式訪問網路。

更改方法：

將金山網路防火牆 V9.0 主介面切換到套用規則頁面。選中要修改其套用規則的套用程式，點擊右側的操作，在彈出的操作中選擇。



4.2.4.4 添加套用規則列表

打開金山網路防火牆 V9.0 的主介面，在金山網路防火牆 V9.0 主介面中，單擊“套用規則”標籤，單擊“套用規則”視窗列表右上部的“添加”圖示 添加 ，並在彈出的視窗中選取想要添加許可權規則的程式，可以看到在“套用規則”視窗中，您想要添加的套用程式的許可權規則已經存在於列表中。

新添加許可權規則的程式，金山網路防火牆 V9.0 對其提出訪問網路請求時所採取的預設操作為“詢問”。

4.2.4.5 刪除套用規則列表

將金山網路防火牆 V9.0 主介面切換到套用程式頁面，單擊“套用規則”視窗列表右上部的“刪除”圖示 刪除 ，彈出是否確認刪除該套用程式訪問許可權的對話方塊，點擊“確定”，在“套用規則”視窗中，剛刪除訪問許可權的套用程式已經不存在於列表中。

4.2.4.6 清空套用規則列表

將金山網路防火牆 V9.0 主介面切換到套用程式頁面。單擊“套用規則”視窗列表右上部的“清空”圖示 清空 ，彈出是否確認刪除全部套用程式訪問許可權的對話方塊。點擊“確定”，在套用程式許可權規則列表中所有程式被清空。

4.2.5 網路狀態

金山網路防火牆 V9.0 的網路狀態功能有助於瞭解當前您的電腦上連接到外部網路的套用程式的詳細資訊，您可以通過查詢網路狀態來找出當前連接到網路的可疑套用程式並結束其進程。

使用網路狀態，您可以查看當前您電腦上連接到外部網路的套用程式的名稱、安裝路徑、使用的 TCP 埠或 UDP 埠，並結束可疑套用程式的進程。

4.2.5.1 當前網路活動狀態列表

打開金山網路防火牆 V9.0 的主介面，單擊“網路狀態”標籤，在“網路狀態”視窗列表中，即可以查看到當前您電腦上連接到外部網路的套用程式的名稱、安裝路徑、使用的 TCP 埠及 UDP 埠，如圖所示：



4.2.5.2 打開程式所在目錄

如果您想要進一步瞭解“網路狀態”視窗中某個連接到外部網路的套用程式，您可以打開該程式所在的目錄進行查看。

打開金山網路防火牆 V9.0 的主介面。在金山網路防火牆 V9.0 主介面中，單擊“網路狀態”標籤。在“網路狀態”視窗列表中，單擊要查看的套用程式，單擊列表上部的“開啓程式所在目錄”圖示。您可以看到該程式所在的目錄視窗被打開，此時可以對該程式進行判斷並進行其他操作。

4.2.5.3 結束可疑進程

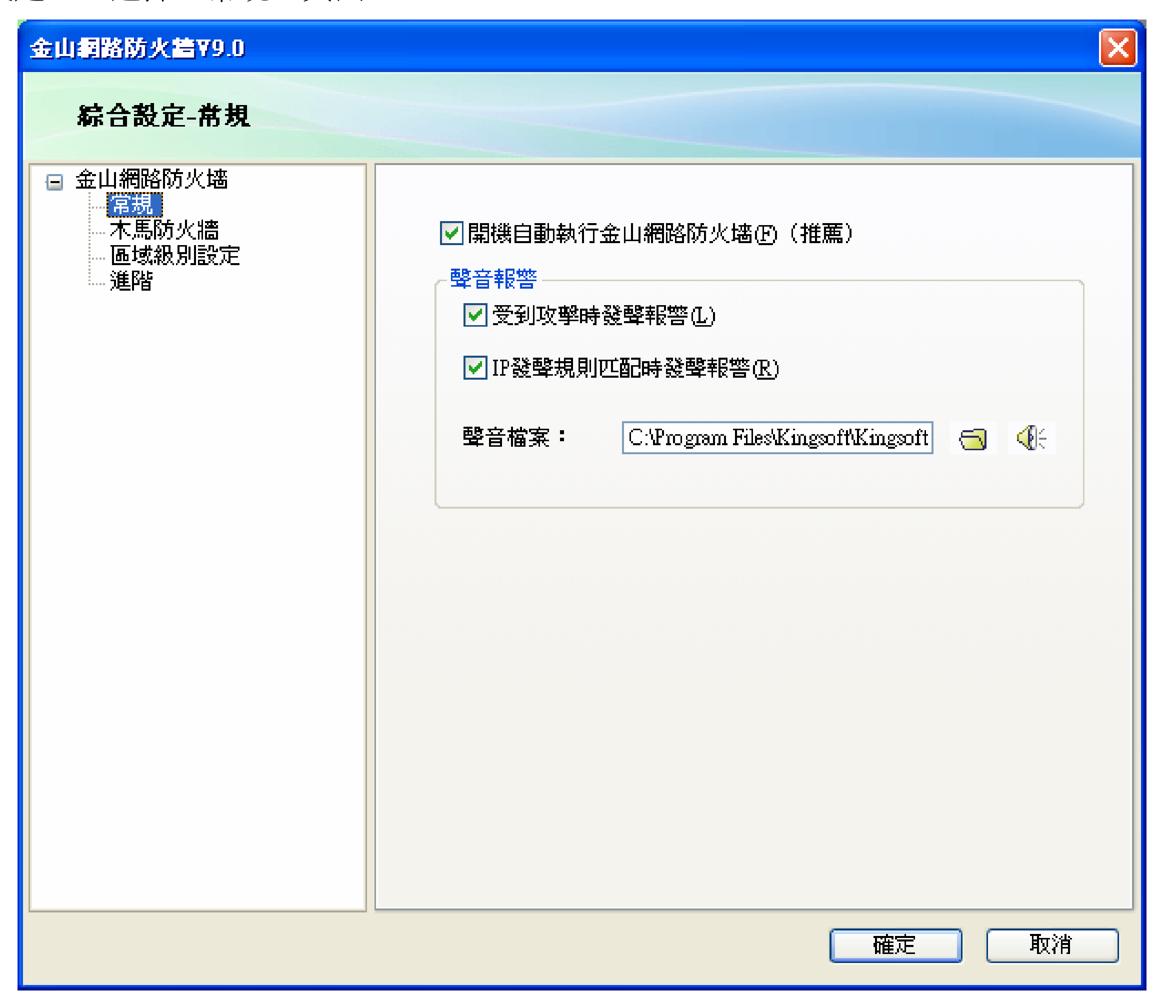
如果您對“網路狀態”視窗中某個連接到外部網路的套用程式感到可疑，您可以結束其進程。

打開金山網路防火牆 V9.0 的主介面。單擊“網路狀態”標籤。在“網路狀態”視窗列表中，單擊可疑的套用程式，單擊列表上部的“關閉程式”圖示，在彈出的窗口中單擊“確認”按鈕。您可以看到在“網路狀態”視窗列表中，可疑的套用程式已經不存在了，即它的網路進程已經被結束。

4.2.6 綜合設定

4.2.6.1 常規設定

點擊金山網路防火牆 V9.0 主介面功能表欄“工具”，在下拉功能表中選擇“綜合設定”，選擇“常規”頁面。



在“常規”頁面中，您可以做如下設定：

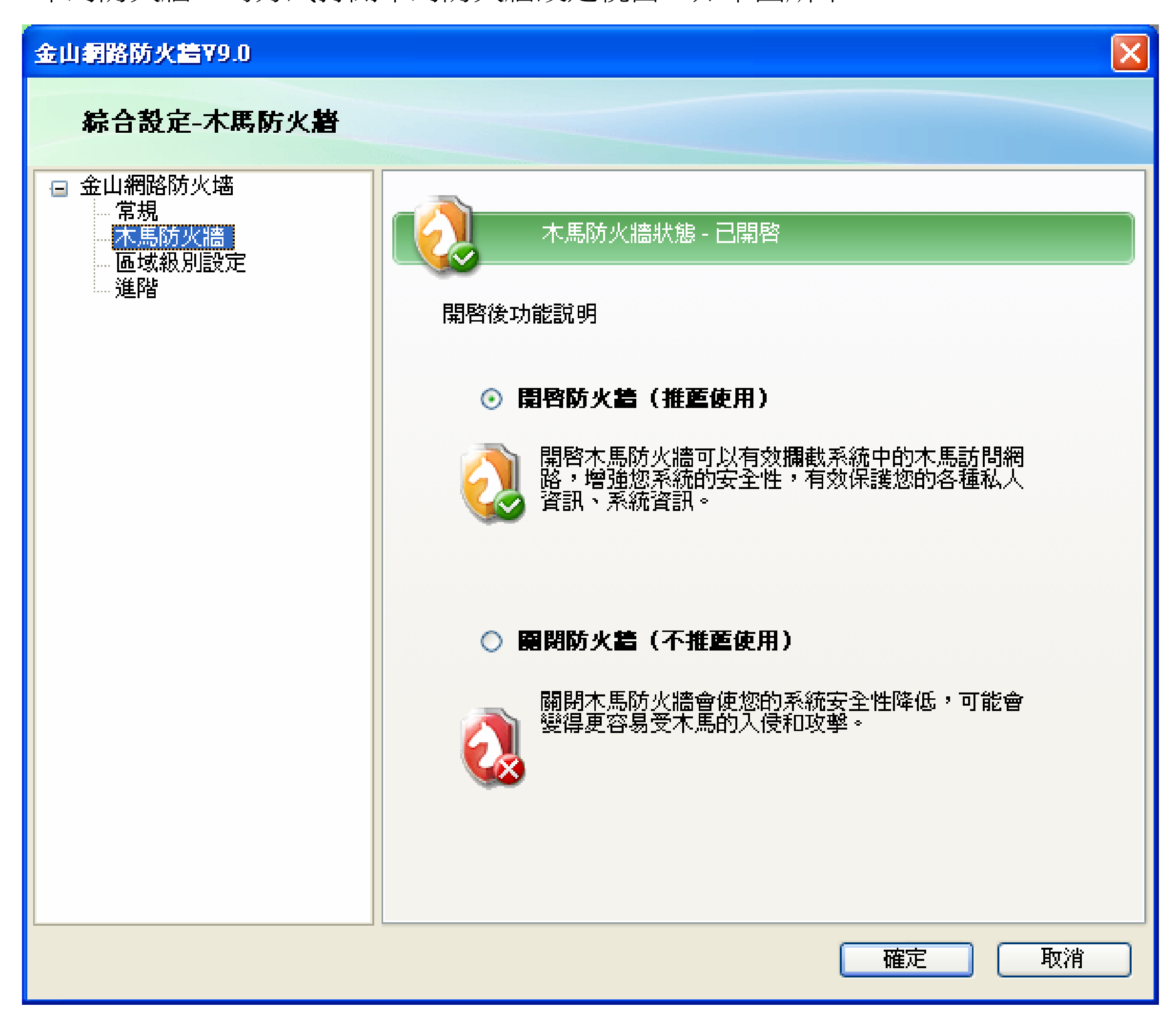
✓ 啟動設定：開機自動運行金山網路防火牆V9.0

✓ 報警設定：當網路出現異常時使用下列聲音報警：用滑鼠單擊此選項前的選擇框，將出現“√”，表示當網路出現異常時，將會使用您設定的音效檔案報警。

4.2.6.2 木馬防火牆設定

系統推薦使用開啟防火牆，因為木馬防火牆可以幫助用戶阻止木馬訪問網路，增強系統的安全性。遇到木馬會自動刪除，無需人工干涉，最大限度的保護您機器的安全。而關閉木馬防火牆，則很容易受到木馬的攻擊。

您可以通過點擊金山網路防火牆 V9.0 主介面功能表欄“工具”→“綜合設定”→“木馬防火牆”的方式打開木馬防火牆設定視窗，如下圖所示：



4.2.6.3 區域級別設定

金山網路防火牆 V9.0 為您的電腦在局域網和互聯網中分別提供了高、中、低三種預設安全級別，同時用戶還可以自定義安全級別。

✓ 預設安全級別

電腦安裝金山網路防火牆 V9.0 之後，金山網路防火牆 V9.0 區域級別設定會採用預設的“中”安全級別來保護您的電腦。可以在“監控狀態”頁面查看。如下圖所示：



用戶可以通過滑杆的滑動來選擇適合高、中、低的安全級別。還可以通過點擊功能表欄的“工具”→“綜合設定”→“區域級別設定”來選擇。“區域級別設定視窗”如下圖所示：



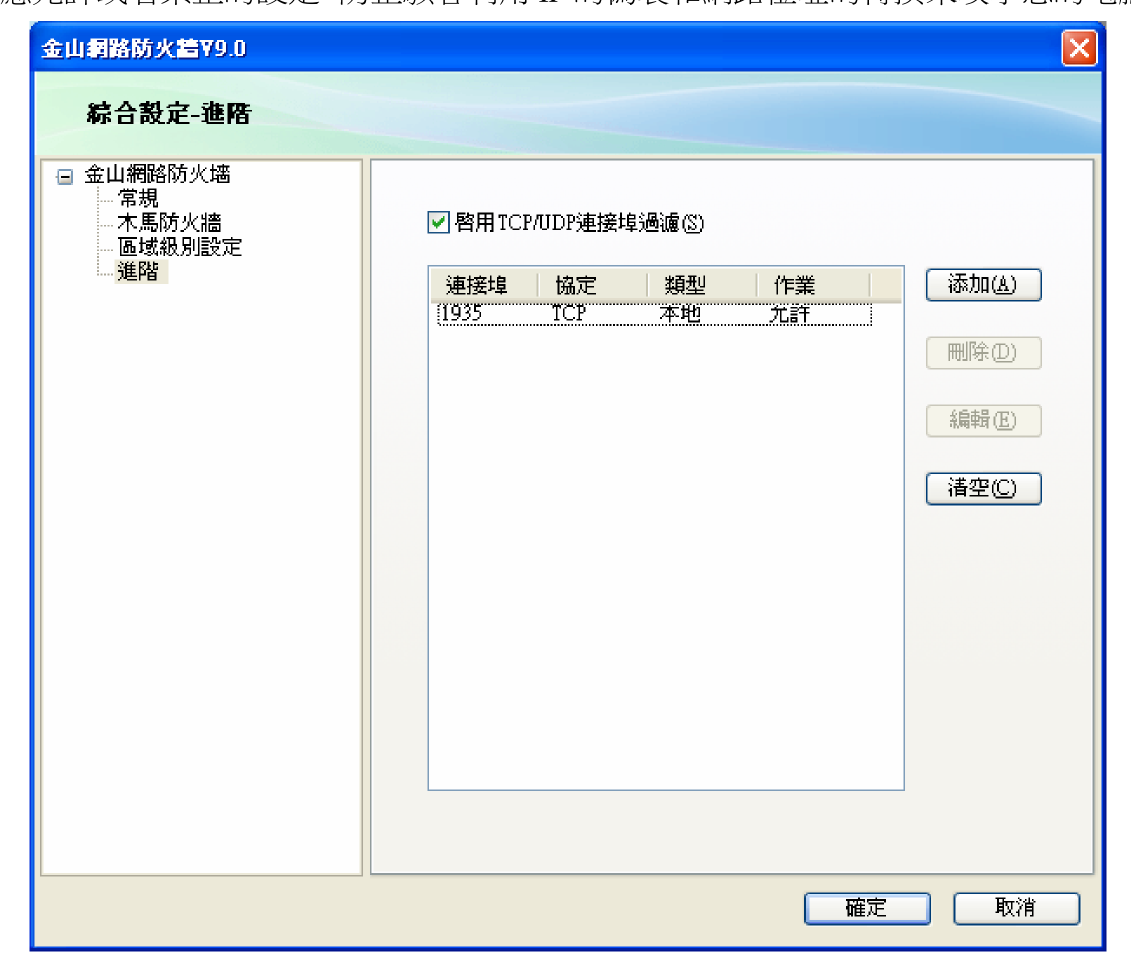
✓ 自定義安全級別

用戶可以通過點擊上圖所示的“自定義級別”按鈕，打開“自定義 IP 規則編輯器”進行相應的設定，還可以通過點擊金山網路防火牆 V9.0 主介面的“監控狀態”在彈出的頁面右側點擊“詳細設定”打開“自定義 IP 規則編輯器”。

【提示】：區域級別設定的詳細說明可參照“監控狀態”下的“安全級別設定”和“自定義 IP 規則”。

4.2.6.4 埠過濾設定

IP 包過濾技術是防火牆技術的基礎。如果您對領域比較熟悉，在“埠過濾”頁面中，可以使用 IP 包過濾技術，手動添加 IP 包過濾規則，對符合條件的 IP 資料包進行相應允許或者禁止的設定。防止駭客利用 IP 的偽裝和網路位址的轉換來攻擊您的電腦。



第五章 金山反間諜 V9.0

5.1 入門篇

5.1.1 主要功能

金山反間諜 V9.0 是一款針對您的電腦系統進行全方面檢查和維護，為您提供修復建議和方法的網路安全工具。它提供強大的惡意軟體查殺、漏洞修補和系統修復的功能，幫助您抵制各種網路惡意軟體的侵襲，及時防範由於未修補系統或軟體漏洞而造成的各種損失。

檢查電腦的網路安全指數

✓ 全面檢查和評估系統的安全狀況，聯機分析系統載入項是否存在安全風險，推薦簡單安全有效的系統清除方案。

查殺惡意軟體

✓ 增強的惡意軟體查殺引擎，能徹底查殺 600 多種惡意軟體、廣告軟體及隱蔽軟體；

✓ 使用“檔粉碎器”和抗 Rootkits 技術，徹底清除使用 Rootkits 技術進行保護和偽裝的 惡意軟體；

✓ 檢查、卸載超過 200 餘種 IE 插件、系統插件；

✓ 一次性清除多種惡意軟體和插件的混合安裝，快速恢復系統，無須重複操作；

✓ 獨創插件信任列表管理，避免誤刪除自己喜愛的有益插件。

漏洞修補

✓ 全面修復 IE 插件和擴展功能，為瀏覽器減負，使您獲得更好的互聯網體驗；

✓ 調整系統啟動項，加速電腦啟動過程；全面診斷您的系統，聯機自動分析未知載入項。

網頁安全防禦

✓ 自動攔截被駭客利用添加惡意代碼的網頁，保護瀏覽器的健康；

✓ 防偽裝技術，對已知及未知的漏洞均能有效的防範。

主動即時預警

✓ 每當有新病毒爆發或互聯網緊急的安全資訊，讓您第一時間獲得最新的消息。

✓ 金山毒霸 V9.0 會不定時地、自動地彈出相關內容的提示氣泡，讓您確切地瞭解網路情況並採取適當的安全措施。

安全百寶箱

✓ 隨身碟病毒免疫工具，輕鬆管理磁片、光碟、隨身碟等自動運行功能，避免被病毒利用進行感染和傳播。

✓ 進程管理，是利用了“互聯網可信認證”技術的進程管理器，能夠即時圖說文字出系統中存在的木馬、 病毒、惡意軟體等可疑與威脅進程，同時加入了詳細的進程描述資訊，幫助您快速到威脅源、管理進程。

✓ LSP 修補工具，修補惡意軟體導致不能上網的問題；

✓ 歷史痕跡清理，避免歷史記錄洩露隱私；

✓ 垃圾檔案清理，提高系統性能，回收浪費的磁碟空間。

5.1.2 啟動金山反間諜 V9.0

執行以下任一項操作，都可以啟動金山反間諜 V9.0：

✓ 在桌面直接雙擊“金山反間諜 V9.0”的圖示。



✓ 在 Windows2000 任務欄中，單擊“開始→程式→金山毒霸 V9.0 網路安全套裝→金山反間諜 V9.0

✓ 在 Windows XP 任務欄中，單擊“開始→所有程式→金山毒霸 V9.0 網路安全套裝→金山反間諜 V9.0

✓ 在 Windows Vista 任務欄中，單擊“開始→程式→金山毒霸 V9.0 網路安全套裝→金山反間諜 V9.0

5.1.3 主介面介紹

金山反間諜 V9.0 的主介面由工具欄、活動頁面和提示欄三個部分組成：



✓ **工具欄**：包括六個活動標籤“網路安全指數”、“惡意軟體查殺”、“漏洞修補”、“系統修復”、“網頁安全防禦” 和“安全百寶箱”。您可以根據自身需要切換活動標籤，同一時間有且只有一個活動標籤。

- **網路安全指數**：您可以在主頁面查看您的電腦系統當前的網路安全指數，健康報告，檢查發現的問題及推薦功能。通過點擊相應的按鈕，您可以針對系統出現的不同問題，進行各項操作。
- **惡意軟體查殺**：您可在此查找並清理可能存在於電腦的惡意軟體、系統插件和信任插件。
- **漏洞修補**：您可在此掃描及修復整個系統中可能存在的安全隱患，包括系統漏洞和共用漏洞。

- **系統修復**：此頁面可以幫您對系統進行更多的安全管理，包括啟動項管理、瀏覽器修復和全面診斷。
- **網頁安全防禦**：保護用戶的瀏覽器，防止您在訪問網頁時感染木馬。
- **安全百寶箱**：多個實用和方便易用的電腦安全工具。包括隨身碟病毒免疫工具、進程管理器 、LSP修補工具、歷史痕跡清理和垃圾檔案清理。

✓ **活動頁面**：隨標籤的變化而不時更換的模組則為活動頁面，在頁面中可以進行各項功能的細則操作和設定。

5.1.4 網路安全指數

金山反間諜 V9.0 啟動後，將自動掃描您電腦中的各個模組，包括惡意軟體，漏洞，殺毒軟體的狀態，可疑檔，未知檔，BHO 和啟動項等，全面檢測並綜合評估您電腦系統的網路安全指數。



根據您電腦的網路安全指數的得分，劃分為四個安全性能級別：

✓ 100 — 86 分

恭喜! 表示您的電腦非常“安全”。當系統只有一些不是很嚴重的小問題，如存在未知檔，啟動項過多等，系統的網路安全指數就會評定在此區間內。

✓ 70 — 85 分

表示系統沒有受到顯著的威脅，但是仍然存在一些影響系統健康因素，稱為“亞健康”狀態。當系統中存在未被信任的風險程式，等級為中等及以下的漏洞（該評定標準是按照微軟發佈的漏洞等級標準），系統盤剩餘的磁碟空間不足，BHO 數量過多等情況，系統的網路安全指數就會評定在此區間內。

✓ 60 — 69 分 黃色警報

表示系統存在顯著的風險，可能感染病毒或遇到嚴重故障。當系統存在可疑檔、等級 4 的惡意軟體（該等級評定標準請參閱：查殺惡意軟體）、嚴重漏洞、或在沒有安裝殺毒軟體等情況下，系統的網路安全指數就會評定在此區間內。

✓ 0 — 59 分 紅色警報

表示系統處於危險當中，用戶有系統崩潰，資料損害或重要資訊洩露的危險。當系統記憶體在病毒、等級 5 的惡意軟體（該等級評定標準請參閱：查殺惡意軟體）、緊急漏洞時，系統的網路安全指數就會評定在此區間內。

5.2 惡意軟體查殺

金山反間諜 V9.0 的惡意軟體查殺功能可幫助您搜尋和清理在未明確提示或未經您許可的情況下，擅自安裝和運行在您的電腦上，侵害您的合法利益的惡意軟體，包括廣告軟體和隱蔽軟體等。同時會進一步管理系統中多餘插件和信任插件。

金山反間諜 V9.0 根據各類惡意軟體的對電腦系統的不同影響制定了由 1 到 5 的危險評分等級。詳細的危險等級評定標準，如下所示：

等級 1：此類為不對電腦系統造成任何威脅的安全軟體。

等級 2：此類為某些有提示捆綁安裝在您電腦上，或者有添加 IE 插件行為，對系統影響不大的惡意軟體。建議繼續保留。

等級 3：此類為有彈出廣告視窗，或劫持瀏覽器，並不提供卸載服務的惡意軟體。建議您使用進行清除。

等級 4：此類為有明顯地彈出廣告窗口，劫持並破壞瀏覽器，危害較大的惡意軟體。建議您立即使用進行清除。

等級 5：此類為有竊取或發佈用戶檔，資訊，盜取任意帳號和密碼，或禁用系統功能，破壞安全模式等的惡意軟體。建議您立即使用進行清除。

5.2.1 查殺惡意軟體

使用方法：

✓ 點擊主介面的“惡意軟體查殺”。

✓ 掃描出您的系統中已經安裝的惡意軟體及詳細說明，包括軟體類別、名稱、出品公司、惡意行為描述及危險級別等。

✓ 選中您想要清除的惡意軟體，點擊“清理選定項”。金山反間諜立即為您進行清理工作。


金山反間諜
金山反間諜 V9.0
毒霸首頁
聯機幫助
網路安全指數
惡意軟體查殺
惡意軟體 (0項)
第三方插件 (0項)
信任插件 (0項)
漏洞修補
系統修復
網頁安全防禦
安全百寶箱
您的系統中已安裝了：
Kingsoft Internet Security
產品主頁
惡意軟體：查殺惡意軟體、廣告軟體、隱蔽軟體
選中狀態
名稱
危險級別
惡意軟體
沒有發現惡意軟體
廣告軟體
沒有發現廣告軟體
隱蔽軟體
沒有發現隱蔽軟體
全選
再次掃瞄
信任選中項
清除選定項


惡意軟體：查殺惡意軟體、廣告軟體、隱蔽軟體
選中狀態
名稱
危險級別
惡意軟體
沒有發現惡意軟體
廣告軟體
WinStdup變種b
出品公司：www.borlander.com.cn
行爲描述：強制安裝、彈廣告、下載隱蔽軟體。
隱蔽軟體
wincdb(RiskWare)
出品公司：未知
行爲描述：彈廣告、下載隱蔽軟體。
異常的Shell
出品公司：未知
行爲描述：非系統默認的Shell啓動之，可能被病毒更改；“移除”恢復至系統默認…
全不選
再次掃瞄
信任選中項
清除選定項

✓ 對於您確定為非危害性的軟體,您可選中該信任軟體，點擊“信任選中項”，該軟體將不會再被認為是惡意軟體。

5.2.2 管理第三方插件

插件是指會隨著 IE 瀏覽器的啟動自動執行的程式,有些插件程式能夠幫助用戶更方便流覽網際網路或調用上網輔助功能，也有部分惡意插件程式監視用戶的上網行為，並把所記錄的資料報告給插件程式的創建者，以達到投放廣告，盜取遊戲或銀行帳號密碼等非法目的。

使用方法：

✓ 點擊主介面的“惡意軟體查殺”→“第三方插件”。

✓ 金山清理專家掃描出您的系統中已經安裝的系統插件及詳細說明，包括軟體類別、名稱、出品公司、惡意行為描述及危險級別等。

✓ 選中您想要清除的第三方插件，點擊“清除選定項”，金山反間諜立即為您進行清理工作。





✓ 對於您確定為不對系統造成危害的第三方插件，您可選中該插件，點擊“信任選中項”，該軟體將不會再被認為是惡意第三方插件。

5.2.3 管理信任插件

金山反間諜 V9.0 的信任插件包括金山反間諜信任的軟體和您信任的軟體兩個專案。金山反間諜信任的軟體是指通過檢測，不對電腦系統造成任何風險的安全軟體。而您信任的軟體是指您已經確定為非危害性的，在之前的操作中已手動將其設定為信任項的軟體。

使用方法：

✓ 點擊主介面的“惡意軟體查殺”→“信任插件”。

✓ 金山反間諜將掃描出您的系統中已經安裝的信任插件及詳細說明，包括軟體類別、名稱、出品公司、惡意行為描述及危險級別等。

✓ 如果您仍想對被掃描出來的插件進行清除，請選中您想要清除的信任插件，點擊“清除選定項”。金山反間諜立即為您進行清理工作。



✓ 對於您確定為非信任插件的系統插件,您可選中該插件，點擊“不再信任選中項”，該軟體將會再次被金山反間諜辨別為惡意軟體。



5.3. 漏洞修補

多數病毒會利用漏洞在互聯網進行傳播，像衝擊波、震盪波、艾妮等。為了避免您因未能及時修復漏洞而造成損失，除了及時到相關網站打上補丁外，你可以使用金山反間諜的漏洞修補功能及時掃描存在于電腦的安全漏洞，並進行安裝補丁程式。

5.3.1 系統漏洞修補

系統漏洞可以是軟體、硬體、程式缺點、功能或配置，也可以是安全隱患。系統漏洞修補功能可以全面掃描整個電腦中可能存在的系統漏洞，並提供該漏洞及補丁的詳細資訊，引導您進行修復操作。

使用方法：

✓ 點擊主介面的“漏洞修補”→“系統漏洞”。



✓ 金山反間諜掃描出您的系統中存在的漏洞及補丁的詳細說明。包括漏洞名稱、補丁發佈時間、大小、安裝需求及危險級別等。

✓ 選中您想要修復的漏洞，點擊“修復選中的漏洞”。



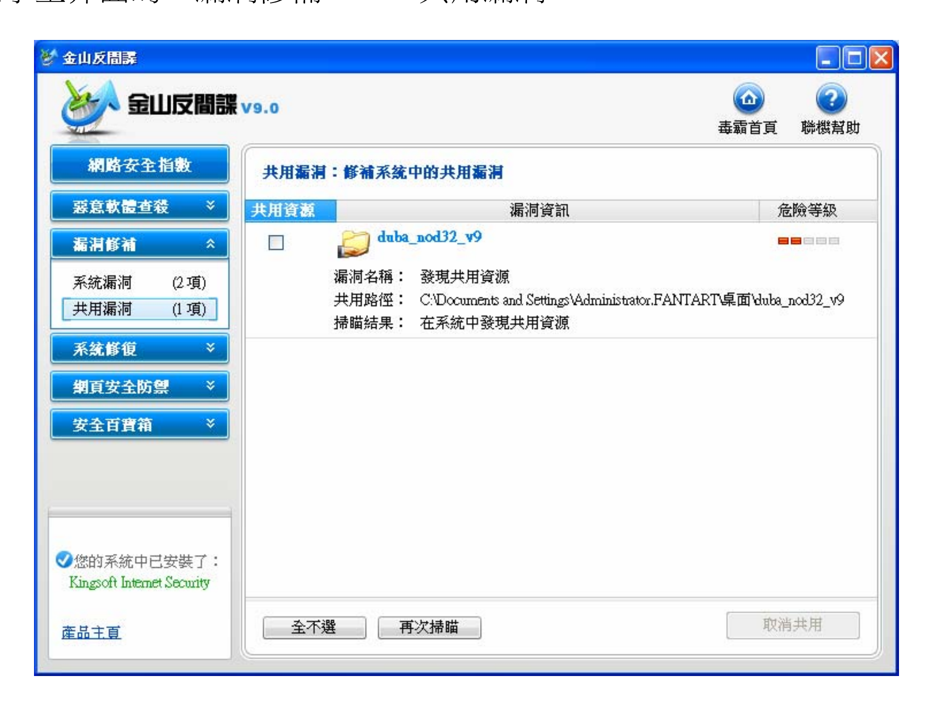
✓ 修復過程開始，請依照提示進行操作，完成修復。

5.3.2 共用漏洞修補

部分病毒可以通過網路共用漏洞隨意進入您的電腦，更可怕的是，駭客可以通過你的電腦實現對這些預設共用的訪問。使用金山反間諜全面檢查整個電腦中存在的共用漏洞，預防病毒趁機偷襲您的電腦，並可瞭解該共用資源的詳細資訊，進行管理操作。

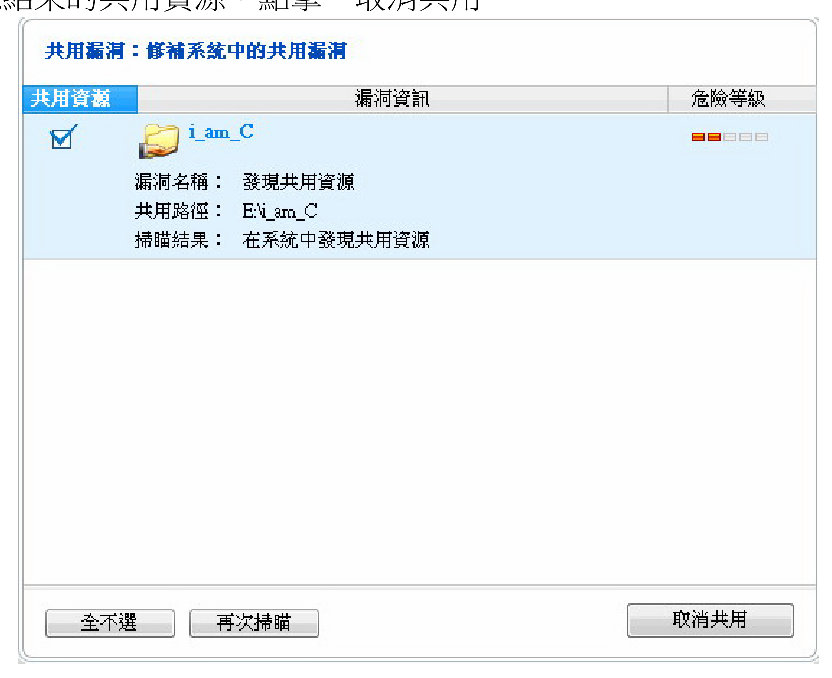
使用方法：

✓ 點擊主介面的“漏洞修補”→“共用漏洞”。



✓ 金山反間諜掃描出您的系統中存在的漏洞及補丁的詳細說明，包括漏洞名稱、路徑和危險等級等。

✓ 選中您想結束的共用資源，點擊“取消共用”。



✓　如果您確定要取消該共用資源，請在彈出的對話方塊裏點擊“是”，完成修復。此資源將不能被局域網內的其他電腦訪問。

5.4 瀏覽器及系統修復

　　隨著電腦使用時間的增長，系統難免會出現各式各樣的問題，金山反間諜 V9.0 的系統修補功能為您提供多個維護系統的實用工具，包括啟動項管理、瀏覽器修補和全面診斷。

5.4.1 啟動項管理

　　金山反間諜 V9.0 的啟動項管理工具可掃描查看當前已經登記的開始功能表啟動項和開機自啟動項，並提供詳盡的說明，包括安全評估、發行商、狀態 、路徑等。讓您可以全面和綜合地查看到系統中是否存在危害性的啟動項。

使用方法：

✓　點擊主介面的“系統修復”→“啟動項管理”。

✓　在活動頁面中，分類列出了各個系統啟動項及詳細說明。

✓　如果您想終止某啟動項功能，請手動選中具體的所需啟動項,點擊“禁用選中項”，即可完成操作。



✓　如果您想重新啟動某些已禁止的啟動項功能，請手動選中具體的所需啟動項,點擊“啟用選中項”，即可完成操作。

5.4.2 瀏覽器修補

當您無意流覽了惡意網頁或惡意腳本可能會修改您電腦的瀏覽器設定和系統的常規項設定。您可以用金山反間諜 V9.0 的瀏覽器修復工具來恢復瀏覽器的設定和擴展功能等。

使用方法：

✓ 點擊主介面的“系統修復”→“瀏覽器修補”。

✓ 金山反間諜 V9.0 自動檢測 IE 中存在的問題,按組別掃描類型和操作建議劃分。您可以結合金山反間諜的安全評估及推薦操作，選擇所需修復項。

✓ 手動選中具體所需的修復項,點擊“修補選中項”。

✓ 如果您確定已瞭解該操作的內容和結果，請在彈出的對話方塊裏點擊“確定”，進行修補。

✓ 點擊“完成”， 修補完畢。

5.4.3 全面診斷

金山反間諜可為您的電腦系統提供最全面的診斷資訊。您還可以通過導出和上報診斷報告，給您的電腦系統提供一個專業分析的橋樑。

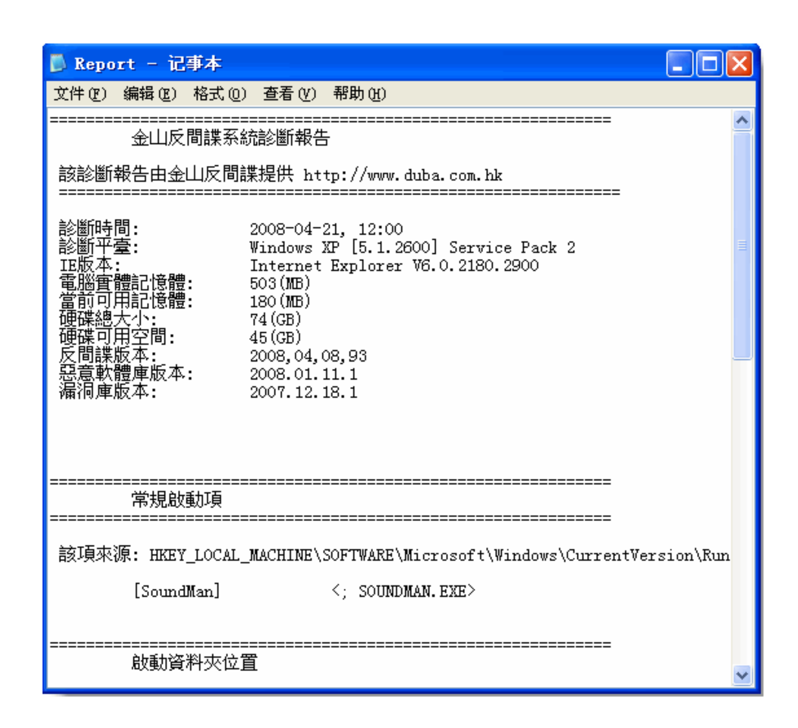
使用方法：

✓ 點擊主介面的“系統修復”→“全面診斷”。

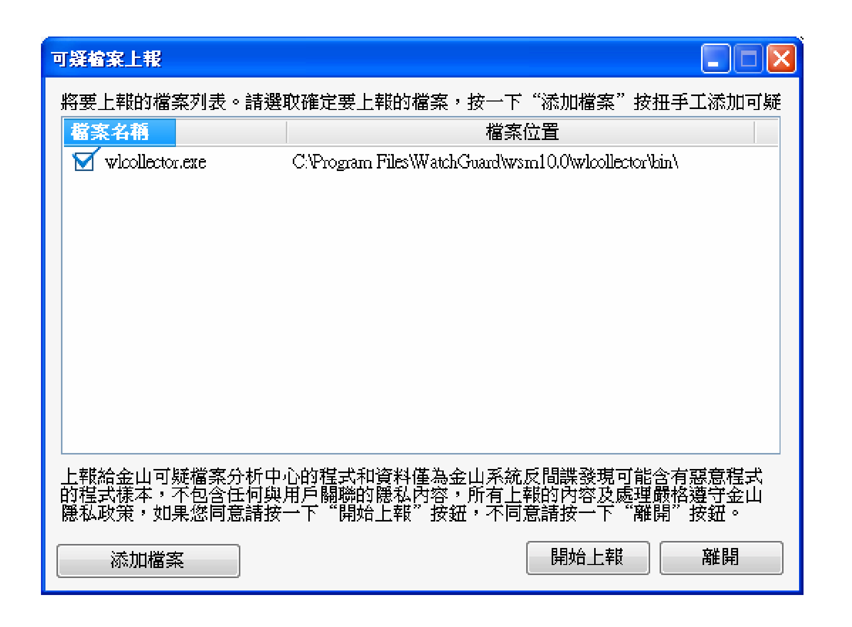


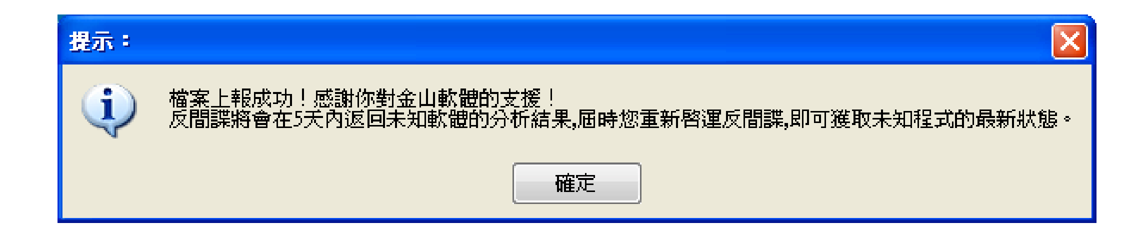
✓ 自動檢測未知載入項。

✓ 如果您想導出該掃描報告，點擊“匯出診斷報告”，在彈出的窗口中獲得診斷報告。



✓ 如果您想重新啟動某些已禁止的啟動項功能，請手動選中具體的所需啟動項,點擊"啟用選中項" ，即可完成操作。





5.5 網頁安全防禦

駭客常常會通過對正常的網頁添加非法代碼，並利用 IE 漏洞進行傳播。當您使用瀏覽器訪問網頁時，瀏覽器便會自動下載木馬程式、病毒和其他惡意程式等到您的電腦上。它們會在您的電腦上進行多種危害性操作，如盜取您的網銀、網遊或 IM 帳號和密碼等，直接危害到您的電腦系統及網路個人資訊的安全。金山反間諜的網頁安全防禦馬功能幫您監控電腦的 IE 瀏覽器，防止您因流覽利用 IE 漏洞注入惡意代碼的網頁而造成的損失，對已知及未知的漏洞均能有效的防範。當遇到此非正常網頁時，金山反間諜的瀏覽器保護功能會自動攔截並給您提示。

網頁安全防禦功能需要在用戶的瀏覽器中安裝插件，一些安全修復工具在掃描您的 ...
...電腦中



日誌查看

在本頁的日誌查看區域，詳細的記錄了每次該功能的操作情況。您可以點擊刷新日誌、清空日誌、列印日誌和導出日誌的鏈結，進行相應的所需的操作。

關閉及卸載

✓ 點擊主介面的“網頁安全防禦”。
✓ 點擊“關閉並卸載”按鈕。
✓ 系統自動進入未啟動網頁網頁安全防禦的頁面，表示該功能已經被關閉並移除。

5.6 安全百寶箱

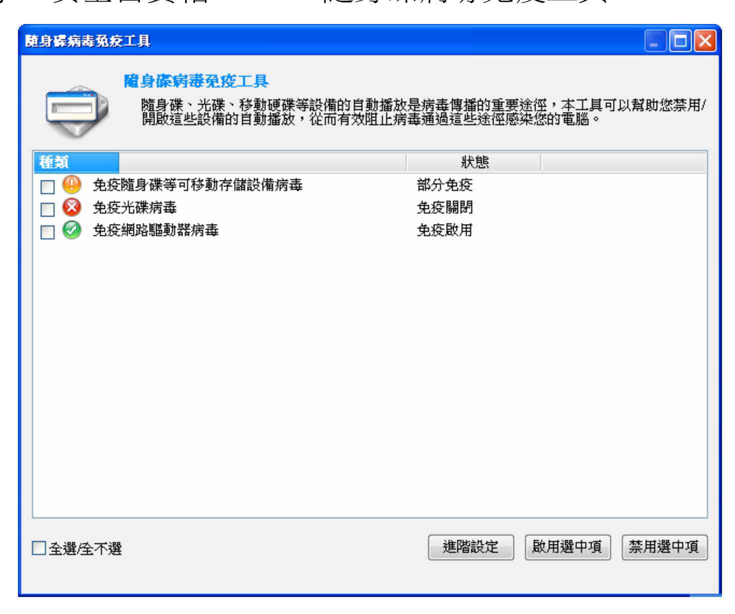
金山反間諜 V9.0 的安全百寶箱沿用了金山反間諜的精髓，結合您的實際需求，進一步為您開發了多個實用和方便易用的電腦安全工具。包括隨身碟病毒免疫工具、進程管理器 、LSP 修補工具、歷史痕跡清理和垃圾檔案清理。

5.6.1 隨身碟病毒免疫工具

自動運行工具，幫助用戶輕鬆管理磁片，光碟，隨身碟等自動運行功能，避免被病毒利用進行感染和傳播。

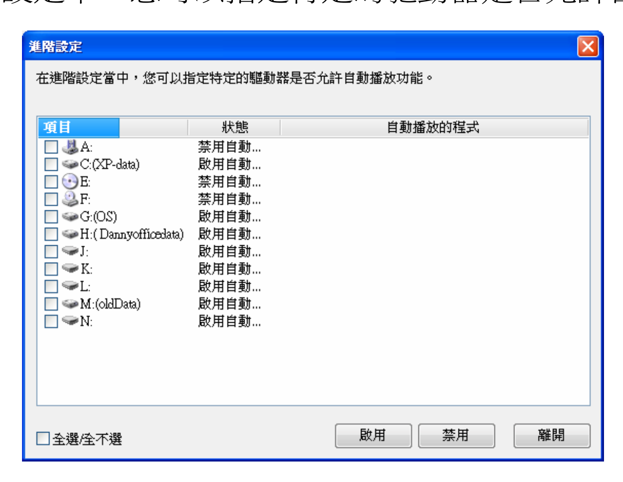
使用方法：

✓ 在主介面點擊“安全百寶箱”→“ 隨身碟病毒免疫工具”。



✓ 在彈出的頁面中，選中一項或多項，點擊“啟用選中項”或“禁用選中項”。

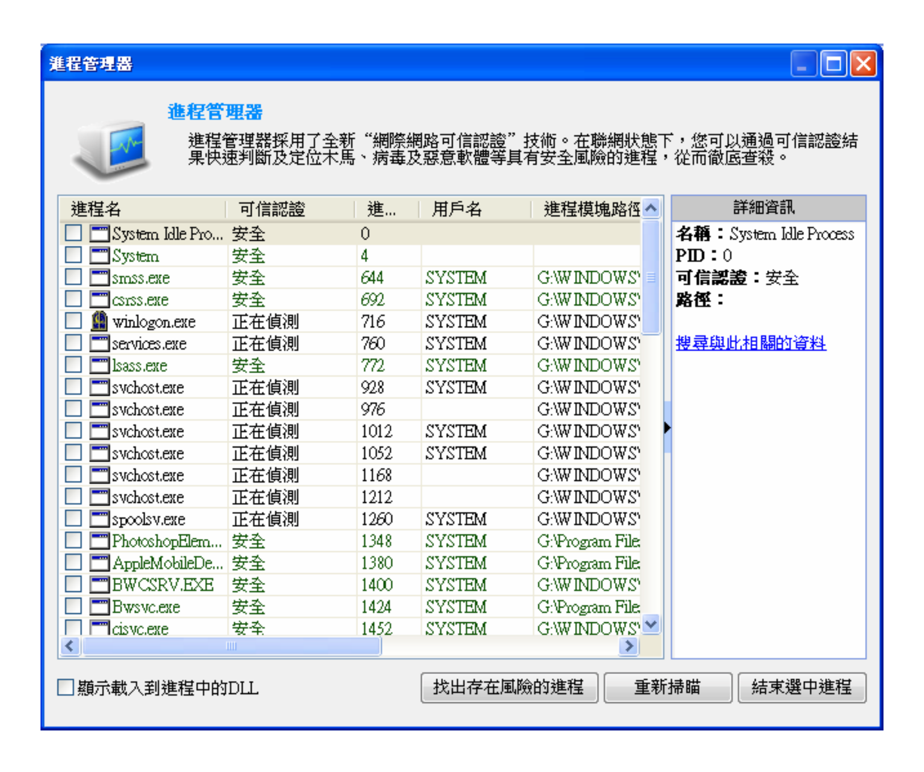
進階設定：在進階設定中，您可以指定特定的驅動器是否允許自動運行功能。



5.6.2 進程管理器

進程管理器，是利用了“互聯網可信認證”技術的進程管理器，能夠即時圖說文字出系統中存在的木馬、 病毒、惡意軟體等可疑與威脅進程，同時加入了詳細的進程描述資訊，幫助您快速到威脅源、管理進程。

1. 在主介面按一下“安全百寶箱”→“進程管理器”。
2. 在彈出的頁面中，可以清楚地看到電腦正在執行的各項進程，對不明進程直接可線上搜尋相關資料，並可對其直接管理。對於“可信認證”中認定的危險進程，建議立即結束。



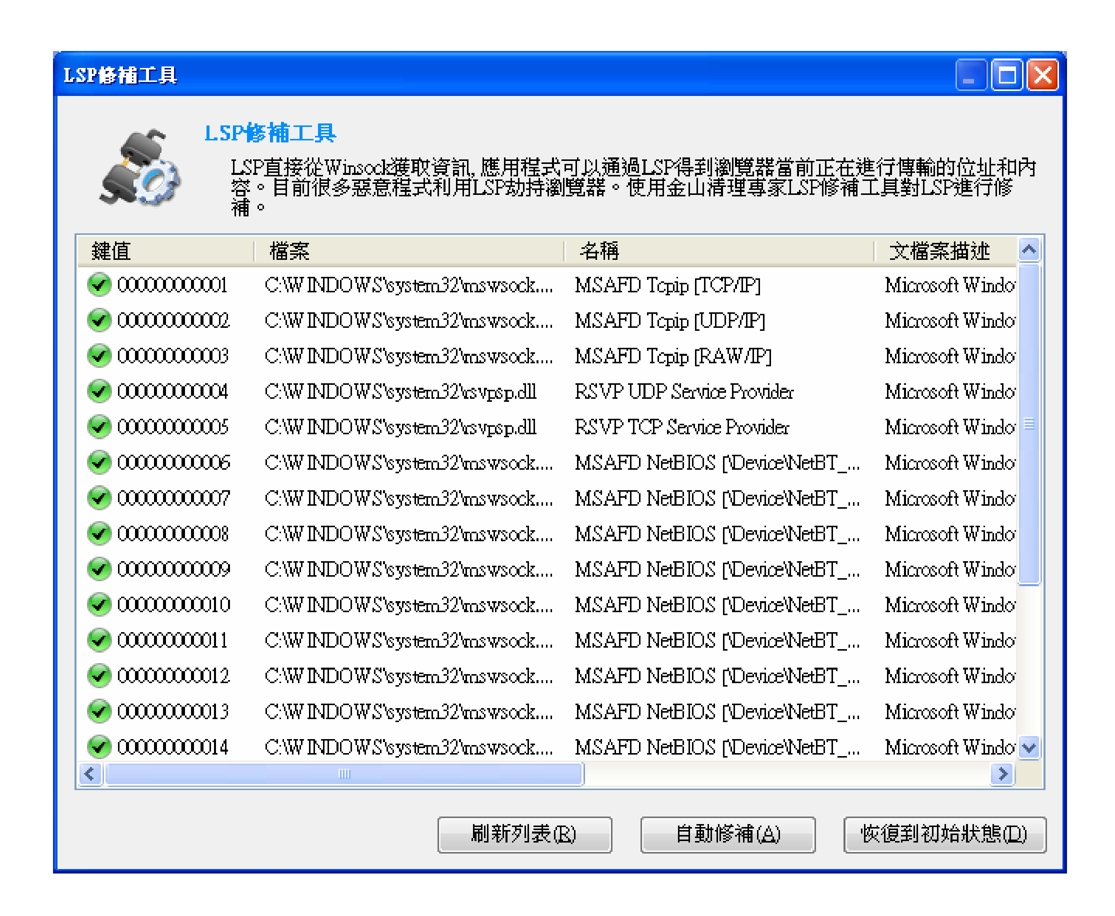
顯示加載到進程中的 dll：選取其中一項或多項，再勾選此複選項可更詳細地檢視、管理進程。

5.6.3 LSP 修補工具

LSP（Layerd Service Provider)，中文名稱為分層服務提供程式，網路管理員可利用它來更好地監視系統網路通訊情況，但目前很多惡意程式利用 LSP 劫持瀏覽器，如著名的 New.Net 插件或 WebHancer 組件。如您在訪問網站時彈出廣告視窗或經常被重定向到其他網站，您可使用金山反間諜 V9.0 的 LSP 修補工具來修補。

使用方法：

- ✓ 在主介面點擊“安全百寶箱”→“LSP 修補工具”。
- ✓ 在彈出的介面中，點擊“自動修補”。



✓ 自動檢測並修補您的 LSP 存在的問題。

【注意】：如果需要將 LSP 恢復到原始狀態，請在彈出的介面中，點擊“恢復到初始狀態”。LSP 修補功能將徹底還原您的 LSP，請在使用前確認。

5.6.4 歷史痕跡清理

歷史痕跡清理工具列出了用戶電腦中以下九項使用記錄：

✓ 使用 IE 時輸入的位址列表
✓ 上網訪問遺留的臨時網頁檔
✓ 開始功能表中曾經訪問過的文檔歷史記錄
✓ 開始功能表中曾經使用過的“運行”歷史記錄
✓ 上網時記錄在本地的 Cookies
✓ Windows 系統中殘存的暫存檔案
✓ 上網訪問歷史記錄
✓ RealOne/RealPlayer 播放表歷史紀錄
✓ Windows 媒體播放器播放表歷史紀錄

使用方法：

✓ 在主介面點擊“歷史痕跡清理”。
✓ 在彈出的介面中，點擊上面板中的專案，下面板顯示相應的列表和資訊。



✓ 在上面板中勾選相應的項目，點擊“立即清除”即可。

【注意】：有些歷史痕跡可能由於系統或軟體佔用不能完全得到清理，如遇到此類情況，請關閉其程式然後再進行嘗試；清理使用 IE 時輸入的位址列表需重新啟動 IE 才能生效；清理開始功能表中曾經使用過的“運行”歷史記錄，需要重新啟動 Windows 才能生效。

5.6.5 垃圾檔案清理

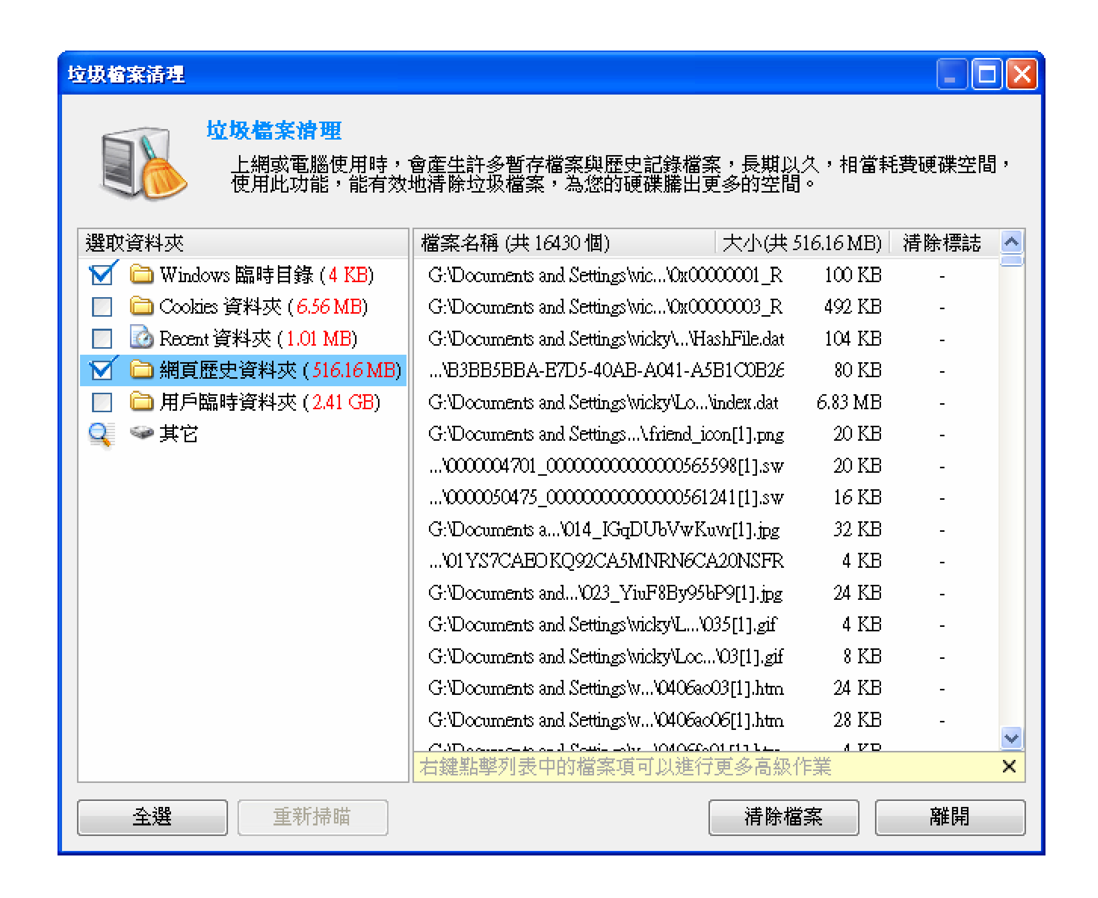
隨著電腦使用時間的延長，垃圾檔會不斷增多，極大地佔用了您的磁碟空間，也影響了系統的運行速度。

使用方法：

✓ 在主介面點擊“安全百寶箱”→“ 垃圾檔案清理”。

✓ 在彈出的介面中，開始檢查存在電腦上的垃圾檔案，包括 Window 臨時目錄、Cookies 檔夾、網頁歷史檔案夾等裏的垃圾文件。

✓ 選中用戶想要清理的專案，點擊“清除檔案”。



✓ 在彈出對話方塊中，顯示成功清除的垃圾檔數量，點擊“確定”，完成清理。

5.7 病毒木馬查殺

為了更好地捍衛您的電腦和互聯網的安全環境，您可通過金山反間諜 V9.0 的病毒木馬查殺選項，獲得最新的安全資訊。

5.7.1 殺毒軟體推薦

增強病毒的防範意識，多流覽相關安全網站，只要您能切實做好安全防範工作，就會盡可能避免因病毒或惡意軟體等帶來的損失。

您可以通過金山反間諜 V9.0 的殺毒軟體推薦頁面，及時瞭解金山毒霸的一些動態，同時可以直接在此頁面免費下載金山毒霸。

第六章　常見問題解答

安裝

1、問：金山毒霸 V9.0 網路安全套裝能安裝在非簡體中文的作業系統上嗎？

答：金山毒霸目前的所有版本只能支援在中文windows系統下安裝運行，如果在其他語言環境的系統中安裝可能會出現程式介面的文字和幫助檔的內容顯示不正常的情況；在英文XP系統中可以通過設定**控制面板—區域和語言選項—中文(香港或台灣)**的方法來臨時解決介面顯示亂碼的問題,但是可能會導致其他原本的英文介面程式顯示異常。

2、問：一套金山毒霸 V9.0 網路安全套裝可以安裝幾台電腦使用？

答：毒霸是單機授權的軟體，僅授權在一台電腦上使用，如果在多台電腦上安裝使用則會被伺服器提示超過授權人數而鎖定。該鎖定一周後自動解除，無法人工解鎖；如果出現此情況建議只在一台電腦上安裝，一周後可恢復正常使用，在服務時間內升級服務不受影響。

3、問：為什麼下載了金山毒霸 V9.0 網路安全套裝後提示需要付費或總是提示服務過期？

答：金山毒霸 V9．0 程式免費提供，可以正常使用，查殺病毒，但相關升級服務（程式更新，病毒庫更新）並不是免費提供的，試用期結束後，需要付費才能更新病毒庫；如果您是盒裝產品用戶，請輸入毒霸正版用戶服務卡序列號進行驗證。

4、問：安裝金山毒霸 V9.0 網路安全套裝後重新啟動電腦出現黑屏白字：“Y：\”的提示是什麼原因，怎麼處理？

答：出現這種情況，請您將金山毒霸的安裝光碟取出，然後重新啟動系統。

5、問：為什麼系統先安裝了金山反間諜，金山毒霸 V9.0 網路安全套裝 就無法安裝呢？

答：金山毒霸 V9．0已經包括了金山反間諜所有的功能，為了避免不必要的衝突，安裝毒霸之前需要先把金山反間諜卸載。

6、問：當金山毒霸 V9.0 網路安全套裝安全起點站頁面中，安全診斷為有風險或有危險，該怎麼做呢？

答：請根據安全起點站頁面上的“安全防禦”和“服務狀態”逐項進行解決。

7、問：為什麼金山毒霸 V9.0 網路安全套裝 安裝完成之後，所有監控都被關閉，如何開啟？

答：導致此問題的原因是您在安裝有其他殺毒軟體或網路防火牆同時存在的同時，又選擇安裝**金山毒霸 V9.0 網路安全套裝** 到您的機器上，為了避免衝突，**金山毒霸 V9.0 網路安全套裝** 會自動將所有監控元件關閉。您可以先卸載其他殺毒軟體或網路防火牆，或者先在系統服務中停掉它們的服務，然後再從**金山毒霸 V9.0 網路安全套**

裝監控和防禦頁面開啟金山毒霸的各項監控以便得到金山毒霸 V9.0 網路安全套裝的全面保護。

8、問：金山網路防火牆 V9.0 支援什麼作業系統？可以在伺服器版作業系統上安裝嗎？

答：金山網路防火牆 V9.0 支持 Windows 2000 professional、Windows XP Professional（32 位）、Windows XP Home（32 位）和 Windows Vista（32 位）的簡體中文、繁體中文、英文和日文的作業系統，不建議在伺服器版本的作業系統中安裝。

9、問：安裝金山網路防火牆 V9.0 的時候需要禁用 Windows XP 或 Windows Vista 自帶的防火牆嗎？

答：在安裝金山網路防火牆 V9.0 之前，我們建議您首先禁用 Windows XP 或 Windows Vista 自帶的防火牆，以防止衝突的出現。

查殺病毒

1、問：如何開啟螢幕殺毒功能？

答：在金山毒霸 V9.0 功能表欄上選擇：工具→綜合設定→殺毒設定→螢幕殺毒，並勾選"將毒霸專用螢幕作為系統當前螢幕"即可。（不支持 Vista）

2、問：金山毒霸 V9.0 可以查殺壓縮包嗎？

答：可以，支援查殺 Zip、Rar、Eml 、LZH 和 7Z 等格式壓縮包。支持 Zip、Rar、Eml 、LZH、7Z、ARJ、cab、tar、chm、gzip 等 10 類壓縮包的查毒。

3、問：金山毒霸 V9.0 一般何時更新病毒庫？

答：金山毒霸 V9.0 每個工作日三次更新病毒庫，如果遇到重大惡性病毒，隨時更新病毒庫。

4、問：如果發現金山毒霸 V9.0 無法查殺的病毒怎麼辦？

答：如果發現了其他反病毒軟體報告為病毒的檔，而金山毒霸 V9.0 並沒有報告，您可以通過 http://up.duba.net/index.shtml 位址提交可疑檔，同時也可以通過金山毒霸 V9.0 主程序工具欄的可疑檔掃描一項提交可疑檔，我們將以最快的速度對可疑檔進行分析。

5、問：如何徹底防止衝擊波及其變種等一類型或者惡郵差等的病毒感染？

答：對於衝擊波及其變種這類利用系統漏洞傳播的病毒，安裝微軟提供的 RPC 漏洞補丁，便可徹底防止利用這漏洞入侵的病毒，如果您不清楚系統是否存在這個漏洞，建議使用金山毒霸 V9.0 的掃描系統，查看掃描結果，即可知道是否存在該漏洞。對於惡郵差等病毒，需要把系統的管理員密碼設定比較複雜，以免被病毒的內置密碼庫猜中而感染病毒。另外需要及時升級金山毒霸 V9.0 ，隨時開啟檔即時監控。

6、問：如果已經安裝上金山毒霸 V9.0 還需下載那些專殺工具嗎？

答：不需要。金山毒霸推出的專殺工具只是針對查殺一種或者及其變種的少數病毒，而對於這些病毒金山毒霸 V9.0 均可徹底進行查殺。

7、問：為何有時在清除 WORD 巨集病毒後，WORD 程式啟動出現錯誤，重裝 OFFICE 後問題仍然出現？

答：這是由於某些 WORD 巨集病毒已經將 WORD 的範本檔 Normal. dot 破壞，即使重裝 OFFICE 也無濟於事，因為 Normal. dot 檔將保留在系統中。因此，請您在清除病毒後，關閉 WORD，在系統中找到該範本檔，並將其刪除。再次啟動 WORD 程式時，它本身會重建一個新的範本檔，這樣您就可放心的使用了。

8、問：使用金山毒霸 V9.0 能否處理諸如彈出廣告、惡意插件等灰色程式？

答：使用金山反間諜 V9.0 可以處理諸如彈出廣告、惡意插件等灰色程式。

9、問：為什麼 Windows XP 系統切換用戶（或多用戶登陸）之後金山毒霸 V9.0 在 Windows 任務通知欄的小圖示為灰色，並提示檔即時防毒不可用？

答：該情況是正常的，在 Windows XP 系統下，因為用戶切換時第一個用戶仍正在使用毒霸，即時監控仍在運行，系統不會二次啟動該服務，所以會顯示在第二用戶身份下金山毒霸為灰色，除非用戶註銷第一個用戶後以第二個用戶登陸系統，顯示才是正常的；當快速切換用戶後，雖然看到金山毒霸是灰色的，其實毒霸還是在工作中的，不用擔心系統不受保護。

10、問：無法正常瀏覽網頁，無論打開任何位址都指向某一個網站。能否使用金山毒霸進行恢復？

答：此情況一般是因為病毒對 ie 的解析檔作了修改，建議嘗試以下操作：修改 C:\WINDOWS\System32\drivers\etc\ 下麵的 hosts 文件。只保留 127.0.0.1 localhost 這行，此行以外的內容，全部刪除就可以解決了，不需要通過毒霸來解決。

11、問：為什麼在使用金山毒霸時在非管理員許可權登錄時不能自動升級？

答：因為按照 windows 系統許可權的設定，特別在 Vista 環境下：在非管理員下不能覆蓋管理員創建的檔案；所以為了避免給用戶帶來麻煩，毒霸程式中設定為非管理員許可權登陸系統是不能進行升級的。

12、問：金山毒霸病毒隔離系統中的檔案該如何處理，是否會對系統安全產生影響？

答：金山毒霸隔離區中檔案為毒霸清除病毒後的備份，不會對影響系統安全。建議將隔離區中檔案清空即可。設定此檔夾的目的：可能有部分檔案對於用戶來說資料非常重要，即使是染毒檔案也要比完全丟失強，所以，如果用戶遇到此種情況，在傳統的殺毒軟體中，如果清除不成功，可能直接刪除了這個檔案；而被毒霸處理的病毒，則會有檔備份，如果這個檔案真的非常重要，在必要的時候，還可以從隔離系統中

還原出來作為應急的使用。

13、問：安裝毒霸後,打開瀏覽器提示正在檢查代理伺服器設定,打開網頁速度很慢怎麼處理？

答：可能有個案用戶出現安裝毒霸後,打開瀏覽器提示正在檢查代理伺服器設定,打開網頁速度很慢.發送郵件都正常的情況；此情況可能是安裝毒霸後修改了系統安全級別，其中 IE 的一項設定被改變導致，可以嘗試如下操作：打開 IE—工具—internet 選項—連接—局域網設定—去掉“自動檢測設定”—確定 即可。

14、問：為何已經啟動了惡意行為攔截，還是無法對惡意行為進行阻止呢？

答：因為惡意行為攔截是基於檔即時防毒的基礎上對惡意行為進行判斷的，所以當檔即時防毒關閉時，惡意行為攔截是無法生效的。同樣的，在綜合設定中“開機自動運行惡意行為攔截”也是要在勾選上“系統啟動時自動載入檔即時防毒”後才生效。

15、問：安裝好金山毒霸 V9.0 **後,為何開機時會顯示：“‘檔即時防毒’未載入!”？**金山毒霸 V9.0 **系統狀態顯示：“‘檔即時防毒’不可用”呢？**

答：該現象一般因為相關服務沒有成功載入的原因；建議右鍵點擊“我的電腦”，選擇“管理”命令，在“電腦管理”對話方塊中選擇“服務和套用程式”中的服務。然後查看 kingsoft antivirus services 狀態是否為自動及已啟動，如果狀態是未啟動調整為啟動即可,若仍無法解決或無此服務，建議重新安裝毒霸以修復該服務；同時該情況也有可能與某些特殊的病毒有關，如果以上操作不能解決問題，建議使用可疑檔掃描工具將可疑檔發送給我們核實。

16、問：在使用金山網路防火牆 V9.0 的過程中，遇到提醒有套用程式要求訪問網路，該怎麼辦？

答：**金山網路防火牆 V9.0** 針對系統的網路層進行監控，每一個套用程式訪問網路都需要獲得**金山網路防火牆 V9.0** 的數位安全簽名才可以訪問網路。如果遇到有套用程式要求訪問網路，首先查看詳細資訊，確認此套用程式訪問網路屬於正常情況，即可允許訪問網路，否則禁止訪問網路。

17、問：金山網路防火牆 V9.0 的各種安全級別的定義是什麼意思？一般來說應該套用什麼樣的網路安全級別？

答：1）高安全級別：對訪問網路的套用程式進行許可權控制；對常見的木馬程式和攻擊進行攔截；提供嚴格控制的網路訪問能力；禁止別人探測/訪問本機。

2）中安全級別（系統預設安全級別）：對訪問網路的套用程式進行許可權控制；對常見的木馬程式和攻擊進行攔截；提供用戶日常適用的網路訪問能力，例如瀏覽網頁，收發郵件等。

3）低安全級別：對訪問網路的套用程式進行許可權控制；對常見的木馬程式和攻擊進行攔截；提供寬鬆自由的網路訪問能力。

4）自定義安全級別：**金山網路防火牆 V9.0** 提供的預設安全級別可以為大多數用戶提供足夠的保護。如果預設的安全級別不適合，可以自定義安全級別，方法是使用安全級別滑塊選擇“自定義級別”。**金山網路防火牆 V9.0** 為您提供了方便的安全

級別自定義功能，使您可以按照自己的需要制定適合自身的安全級別。如果是個人普通用戶，建議使用“中”安全級別。(預設為即為“中”安全級別，無須更改) 。

18、問：金山網路防火牆 V9.0 可以有效防範衝擊波(Worm.MSBlast.6176)、蠕蟲王(Worm.SQLexp.376)病毒的攻擊嗎？

答：可以。只要安裝並打開了**金山網路防火牆** V9.0，就可以在沒有打上系統 RPC 漏洞補丁、SQL 補丁的情況下有效攔截衝擊波、蠕蟲王病毒的網路攻擊。但是出於安全考慮，建議最好能為電腦系統打上微軟提供的相關補丁。

19、問：如何可以利用金山網路防火牆 V9.0 有效的防範網路的各類攻擊呢？

答：在安裝了 Windows 作業系統以後，可以運行**金山網路防火牆** V9.0 的漏洞掃描程式，對系統的漏洞進行掃描，通過查看漏洞掃描報告，可以把已知的作業系統漏洞補上。另外可以通過查看漏洞掃描報告發現系統存在的一些安全漏洞，比如共用的設定、系統管理員的密碼等，可以適當對這些漏洞進行設定，從而提高系統的安全性。之後在上網的時候需要打開**金山網路防火牆** V9.0，一般情況下可以設定為預設的中安全級別即可。根據網路環境以及自身需要，還可以及時調整**金山網路防火牆** V9.0 的安全級別以及自定義規則來更好的防範各類網路攻擊。

20、問：在無線的局域網中可以使用金山網路防火牆 V9.0 防範各類網路攻擊嗎？

答：可以。**金山網路防火牆** V9.0 支援 Intel 迅馳技術的網路安全防護產品，特別針對 Intel 的迅馳技術作出了優化處理，能夠在無線的局域網中為個人電腦提供全方面的網路安全防護。

21、問：在使用金山網路防火牆 V9.0 的過程中，遇到提醒有套用規則要求訪問網路，該怎麼辦？

答：**金山網路防火牆** V9.0 針對系統的網路層進行監控，每一個套用規則訪問網路都需要獲得**金山網路防火牆** V9.0 的數位安全簽名才可以訪問網路。如果遇到有套用規則要求訪問網路，首先查看詳細資訊，確認此套用規則訪問網路屬於正常情況，即可允許訪問網路，否則禁止訪問網路。

升級

1、問：當線上升級時出現下載檔案失敗如何處理？

答：當升級時候出現下載檔案失敗，金山毒霸 V9.0 的升級程式將不更新本地的毒霸版本，這可能是由於您的網路環境或伺服器設定的原因造成的，請檢查您是否使用代理伺服器上網。

2、問：引擎不經常升級，是否可以查殺最新病毒呢？

答：可以查殺新病毒。金山毒霸 V9.0 的病毒庫更新以後就可以查殺新出現的病毒，並不一定每次都需要更新引擎。如果出現引擎版本的更新可能會是修正一些錯誤、提

高某些性能等方面的改進，所以引擎並不是經常更新的模組。

3、問：為什麼點擊金山毒霸線上升級時,升級程式一閃而過,無法自動升級？

答：該情況可能是因為毒霸升級程式意外損壞或者被某些程式遮罩導致。

1）首先建議您嘗試將毒霸安裝目錄中的 uplive.exe 改名後（如改名為：1234.exe）重新雙擊這個重命名後的程式開始升級，並在升級後對“我的電腦”進行全面殺毒；

2）如果重命名後仍不能打開 UPLIVE 程式，則有可能是毒霸程式損壞，建議修復安裝毒霸嘗試；

3）如果以上方案都不能解決您的問題，則建議您使用可疑檔掃描工具提交可疑程式給我們以確認是否有新病毒的干擾導致毒霸升級模組不能正常工作。提交後，我們將儘快分析，並更新病毒庫以解決這個問題。

4、問：金山毒霸 V9.0 **升級及驗證採用的埠是什麼？是否可以支援代理升級？**

答：金山毒霸 V9.0 目前驗證及下載升級檔均採用 80 埠，可支援大部分代理軟體正常升級（例如 CCproxy、ISA、Sygate 等）。

5、問：金山網路防火牆 V9.0　提供線上升級嗎？

答：提供線上升級。**金山網路防火牆 V9.0** 會不定期的提供線上升級。通過升級可以修正**金山網路防火牆 V9.0** 的規則檔、更新**金山網路防火牆 V9.0** 的程式，通過升級**金山網路防火牆 V9.0** ，可以攔截比如衝擊波、衝擊波剋星等這類通過網路進行大規模攻擊的病毒。

其他

1、問：日誌檔有什麼用處？

答：日誌檔是用來記錄用戶操作、查毒結果和監控結果的檔。通過日誌檔可以清楚的知道以前本機曾經感染的病毒，以及處理方式，方便追查病毒來源。具體操作請參見日誌檔。

2、問：在資源管理器中拷貝多個檔時發現病毒，為什麼出現無法繼續拷貝檔的情況？

答：由於檔即時防毒在發現病毒需提示時，先返回錯誤碼給系統，保證病毒檔不進入記憶體，然後通知用戶處理；由於資源管理器在拷貝多個檔案時，只要有一個檔案拷貝失敗，則整個拷貝操作失敗，無法繼續拷貝。

3、問：為何在進行磁片碎片整理等磁片操作中有時會出現死機現象？

答：當用戶對磁片進行碎片整理等操作的同時，金山毒霸檔即時防毒處在啟動狀態，也會對磁片進行病毒掃描，兩者操作的速度發生差距，即會導致系統死機，建議您在進行此類操作（如刪除或拷貝大量檔時），暫停或關閉即時防毒。具體操作請參見**檔案即時防毒**。

駭客的攻擊過程

- 資訊收集

駭客儘量多地收集關於您的電腦的資訊。他試圖找到漏洞，讓您察覺不到您的電腦已受到攻擊。

—— 如果駭客已選擇了特定的目標，通過 Internet，駭客可以瞭解可能目標的大量資訊。

—— 如果駭客沒有明確的目標，有許多工具都可以用來掃描 Internet 並查找可能的目標。最簡單的是 ping 掃描，它可以迅速掃描數以千計的電腦 。駭客使用程式來 ping 具有一系列 IP 位址的電腦。如果有回應，說明存在具有該 IP 位址的電腦。

- 初始訪問

駭客利用在收集資訊過程中找到的漏洞，建立進入您的電腦的入口點。

—— 駭客訪問 Windows 電腦的最簡便方法就是使用 Microsoft 網路。許多電腦上都啟用了 Microsoft 網路，因此網路上的任何人都可以連接到該電腦。

- 增加許可權

一旦駭客連接到您的電腦，下一步就是獲得對您電腦上更多程式和服務的訪問許可權。

—— 通常駭客會試圖通過破解密碼獲得對該電腦的管理許可權。駭客會下載密碼檔，並對其進行解碼。

—— 另一個策略是將特洛伊木馬放置到您的電腦上。

- 隱蔽蹤跡

駭客隱藏或刪除入侵證據，有時會保持入口點打開以便返回。

—— 在運行 Windows 2000/XP 的電腦上，駭客會試圖關閉審計功能，並修改或清除事件日誌。在所有電腦上，駭客都會隱藏檔以供他們將來訪問時使用。在極端情況下駭客可能會格式化受到攻擊的電腦的硬碟以避免被識別。

病毒和木馬

- 木馬

一種破壞性程式，經常偽裝成有用或有趣的內容來對電腦進行破壞。

木馬不進行複製，但會危及電腦安全。它偽裝成有用的軟體進行傳播，有些木馬在運行它的電腦上執行惡意操作，有些則為駭客提供遠端控制能力。

- 病毒

一種程式或代碼，它可以通過將其自身附加到另一個程式、引導區、分區或支援宏的文檔進行複製。有些病毒只是複製，有些則會產生破壞。病毒可以隨時通過電子郵件接收的文檔傳播。

網路協定解說

IP(Internet Protocol)用於通過網路傳送 TCP 或者 UDP 發送的資訊。它決定發送的路徑和位址，而且這個位址必須是唯一的，之所以使用唯一位址，是考慮到網路上的所有裝置。為了連接和使用通信網就要把各個獨立的協定連接起來。

ICMP（Internet Control Message Protocol）網間控制報文協議。這個協定在網路中檢測伺服器狀態資訊，能夠不停的運行。它比 TCP/IP 又高了一階層。可以認為 ICMP 是與 IP 在一個相同的階層上的協定，用於處理錯誤資訊。傳送資料的時候，會發生找不到接收地點，或者資料出現異常的現象，如果出現這種現象，ICMP 就會把這一情況告知傳送的郵件。Ping 是 ICMP 的代表性程式 ARP（Address Resolution Protocol）& RAPA

（Reverse Address Resolution Protocol）位址解析協定和反向位址解析協定。

TCP/UDP TCP（Transmission Control Protocol）是面向連接（connection_oriented）的協定和 UDP（User Datagram Protocol）是非面向連接（connectionless）的協定。TCP 是傳輸控制協定，UDP 是用戶資料包協定。

TCP 的標誌位元由 8 位元組成：

URG：表示報頭的 urgent Pointer field 有效

ACK：對於接受到的 segment 進行應答

PSH：將接收到 TCP 緩衝器中的資料立刻向上階層發送

RST：對連接進行初始化（也可以在拒絕連接時使用）

SYN：嘗試連接

FIN：連接結束

第七章 附錄

技術支援

您在使用《金山毒霸 V9.0 網路安全套裝》的過程中遇到的大部分問題，可以在用戶手冊和軟體幫助系統中獲得相應有用的資訊和幫助，如果還是沒有您所需要的資訊，請與我們的技術支持聯繫，我們會以最快的速度回復您一切的問題。您可以通過下列途徑獲得滿意的答復。

服務方式：

一：自助線上搜索或查詢。

登錄 http://www.duba.com.hk 網站可以根據問題的關鍵字進行搜索，查找相關問題的解決方法。或者在常見問題的知識庫中進行查詢。

二：線上問題提交

相關問題登錄：http://support.kingsoft.com 選擇相應的產品及問題，並輸入詳細的相關資訊及 問題的詳細描述通過線上的方式進行提交，我們的工程師將儘快的進行答復。

三 ：技術支持：

香港客戶服務電話：852-26114144
台灣客戶服務電話：886-2-22448452
香港技術支持郵箱：supporthk@kingsoft.com
台灣技術支持郵箱：supporttw@kingsoft.com